

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2003-44297

(P2003-44297A)

(43)公開日 平成15年2月14日(2003.2.14)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 9/46	3 4 0	G 0 6 F 9/46	3 4 0 F 5 B 0 1 7
	3 6 0		3 6 0 D 5 B 0 8 2
1/00	3 7 0	1/00	3 7 0 E 5 B 0 9 8
12/00	5 3 7	12/00	5 3 7 A
12/14	3 1 0	12/14	3 1 0 K
審査請求 未請求 請求項の数56 O L (全 36 頁)			

(21)出願番号 特願2001-322437(P2001-322437)

(22)出願日 平成13年10月19日(2001.10.19)

(31)優先権主張番号 特願2000-352113(P2000-352113)

(32)優先日 平成12年11月20日(2000.11.20)

(33)優先権主張国 日本(J P)

(31)優先権主張番号 特願2001-161403(P2001-161403)

(32)優先日 平成13年4月23日(2001.4.23)

(33)優先権主張国 日本(J P)

(31)優先権主張番号 特願2001-190445(P2001-190445)

(32)優先日 平成13年5月22日(2001.5.22)

(33)優先権主張国 日本(J P)

(71)出願人 500083226

ハミングヘッズ株式会社

東京都中央区月島1丁目2番13号

(72)発明者 大江 尚之

東京都中央区月島一丁目2番13号 ハミン

グヘッズ株式会社内

(72)発明者 志摩 貴浩

東京都中央区月島一丁目2番13号 ハミン

グヘッズ株式会社内

Fターム(参考) 5B017 AA03 BA06 CA16

5B082 EA11

5B098 AA03 AA05 GA02 GA04 GD01

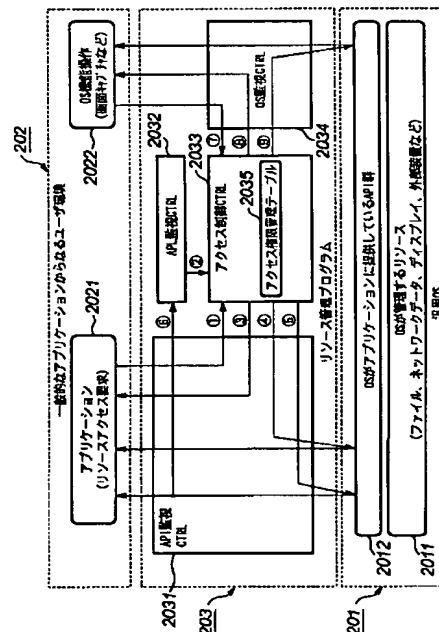
GD03 GD07 GD14 GD21

(54)【発明の名称】 コンピュータリソースの制御を行なう情報処理方法および装置、情報処理システム及びその制御方法並びに記憶媒体、プログラム

(57)【要約】

【課題】 OSやプロセスを変更することなく、アクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張することを目的とする。

【解決手段】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のOSが管理しているコンピュータリソースに対するプロセスまたはOSからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにOSに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するか、コンピュータリソースの内容に応じて課金する事によって許可する。



【特許請求の範囲】

【請求項 1】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理方法であって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程と、

前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程とを備えることを特徴とする情報処理方法。

【請求項 2】 前記捕捉工程は、更に、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉することを特徴とする請求項 1 に記載の情報処理方法。

【請求項 3】 前記判定工程は、特定のコンピュータリソースを指定するリソース指定情報、アクセス権限が有効となる条件情報、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を含むアクセス権限管理テーブルを参照して、アクセス権限があるか否かを判定することを特徴とする請求項 1 に記載の情報処理方法。

【請求項 4】 前記判定工程は、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を参照して、アクセス権限があるか否かを判定することを特徴とする請求項 1 に記載の情報処理方法。

【請求項 5】 前記判定工程は、アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定することを特徴とする請求項 1 に記載の情報処理方法。

【請求項 6】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面キャプチャ権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 3 または請求項 4 に記載の情報処理方法。

【請求項 7】 前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返すことを特徴とする請求項 1 に記載の情報処理方法。

【請求項 8】 前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返すことを特徴とする請求項 1 に記載の情

報処理方法。

【請求項 9】 前記拒否工程は、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すことを特徴とする請求項 1 に記載の情報処理方法。

【請求項 10】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理装置であって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉手段と、

前記捕捉手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定手段と、

前記判定手段の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理手段と、

前記判定手段の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否手段とを備えることを特徴とする情報処理装置。

【請求項 11】 前記捕捉手段は、更に、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉することを特徴とする請求項 10 に記載の情報処理装置。

【請求項 12】 前記判定手段は、特定のコンピュータリソースを指定するリソース指定情報、アクセス権限が有効となる条件情報、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を含むアクセス権限管理テーブルを参照して、アクセス権限があるか否かを判定することを特徴とする請求項 10 に記載の情報処理装置。

【請求項 13】 前記判定手段は、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を参照して、アクセス権限があるか否かを判定することを特徴とする請求項 10 に記載の情報処理装置。

【請求項 14】 前記判定手段は、アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定することを特徴とする請求項 10 に記載の情報処理装置。

【請求項 15】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面キャプチャ権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 12 または請求項 13 に記載の情報処理装置。

【請求項 16】 前記拒否手段は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通

知を要求元プロセスに返すことを特徴とする請求項 10 に記載の情報処理装置。

【請求項 17】 前記拒否手段は、要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返すことを特徴とする請求項 10 に記載の情報処理装置。

【請求項 18】 前記拒否手段は、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すことを特徴とする請求項 10 に記載の情報処理装置。

【請求項 19】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するプログラムコードを記憶した記憶媒体であって、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、
前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、
前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、
前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備えることを特徴とする記憶媒体。

【請求項 20】 前記捕捉工程は、更に、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉することを特徴とする請求項 19 に記載の記憶媒体。

【請求項 21】 前記判定工程は、特定のコンピュータリソースを指定するリソース指定情報、アクセス権限が有効となる条件情報、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を含むアクセス権限管理テーブルを参照して、アクセス権限があるか否かを判定することを特徴とする請求項 19 に記載の記憶媒体。

【請求項 22】 前記判定工程は、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を参照して、アクセス権限があるか否かを判定することを特徴とする請求項 19 に記載の記憶媒体。

【請求項 23】 前記判定工程は、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定することを特徴とする請求項 19 に記載の記憶媒体。

【請求項 24】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面キャプチャー権限、使用プロ

セスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 21 または請求項 22 に記載の記憶媒体。

【請求項 25】 前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返すことを特徴とする請求項 19 に記載の記憶媒体。

【請求項 26】 前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返すことを特徴とする請求項 19 に記載の記憶媒体。

【請求項 27】 前記拒否工程は、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すことを特徴とする請求項 19 に記載の記憶媒体。

【請求項 28】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスの制御をコンピュータに機能させるためのプログラムであって、

20 前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、
前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、
前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、
前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備えることを特徴とするプログラム。

【請求項 29】 前記捕捉工程は、更に、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉することを特徴とする請求項 28 に記載のプログラム。

【請求項 30】 前記判定工程の判定の結果、アクセス権限がないと判定され、前記拒否工程によってアクセスを拒否された場合、課金することによってアクセス権限を許可することを特徴とする請求項 28 に記載のプログラム。

【請求項 31】 前記コンピュータリソースは、ウェブキャスト、デジタル放送、音楽配信等のコンテンツを含むことを特徴とする請求項 28 に記載のプログラム。

【請求項 32】 第 1 端末と第 2 端末とが通信網を介して相互に接続されて構成される情報処理システムであって、

50 前記第 1 端末は、

前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉手段とを備え、

前記第2端末は、

前記捕捉手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定手段と、

前記判定手段の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理手段と、

前記判定手段の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否手段とを備えることを特徴とする情報処理システム。

【請求項33】 第1端末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムの制御方法であって、

前記第1端末において、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程と、

前記第2端末において、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程とを備えることを特徴とする情報処理システムの制御方法。

【請求項34】 第1端末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムの制御のプログラムコードを記憶した記憶媒体であって、

前記第1端末において、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、

前記第2端末において、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備えることを特徴とする記憶媒体。

【請求項35】 第1端末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムの制御をコンピュータに機能させるためのプログラムであって、

前記第1端末において、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、

前記第2端末において、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備えることを特徴とするプログラム。

【請求項36】 通信網を介して他の端末と接続する情報処理装置であって、

前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉手段と、

前記操作要求に対する回答を受信する受信手段とを備えることを特徴とする情報処理装置。

【請求項37】 通信網を介して他の端末と接続する情報処理装置であって、

当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定手段と、

前記判定手段の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理手段と、

前記判定手段の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否手段とを備えることを特徴とする情報処理装置。

【請求項38】 通信網を介して他の端末と接続する情報処理装置の情報処理方法であって、

前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程と、

前記操作要求に対する回答を受信する受信工程とを備えることを特徴とする情報処理方法。

【請求項39】 通信網を介して他の端末と接続する情

報処理装置の情報処理方法であって、
当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程とを備えることを特徴とする情報処理方法。

【請求項 40】 通信網を介して他の端末と接続する情報処理装置の情報処理のプログラムコードを記憶した記憶媒体であって、
前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、

前記操作要求に対する回答を受信する受信工程のプログラムコードとを備えることを特徴とする記憶媒体。

【請求項 41】 通信網を介して他の端末と接続する情報処理装置の情報処理のプログラムコードを記憶した記憶媒体であって、

当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備えることを特徴とする記憶媒体。

【請求項 42】 通信網を介して他の端末と接続する情報処理装置の情報処理をコンピュータに機能させるためのプログラムであって、

前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、

前記操作要求に対する回答を受信する受信工程のプログラムコードとを備えることを特徴とするプログラム。

【請求項 43】 通信網を介して他の端末と接続する情報処理装置の情報処理をコンピュータに機能させるためのプログラムであって、

当該情報処理装置のコンピュータリソースにアクセスす

10

る前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、

前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備えることを特徴とするプログラム。

【請求項 44】 電子情報を変換して操作を制限する情報処理装置であって、

電子情報を読み込み記憶する記憶手段と、

前記電子情報に対する操作を制限する内容を定義した制限属性情報を、前記該電子情報に付加する第 1 付加手段と、

前記電子情報に対する操作を監視し制御する制限プログラムを、前記該電子情報に付加する第 2 付加手段と、

20

前記第 1 及び第 2 付加手段によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力手段とを備えることを特徴とする情報処理装置。

【請求項 45】 実行可能形式データを利用する情報処理装置であって、

電子情報に対する操作を制限する内容を定義した制限属性情報及び電子情報に対する操作を監視し制御する制限プログラムが付加された電子情報を含む実行可能形式データを起動する起動手段と、

30

前記制限プログラムから前記電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込手段と、

前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得手段と、

前記取得手段で取得したアプリケーションを起動するアプリケーション起動手段と、

前記アプリケーション起動手段によるアプリケーションの起動が成功したかどうかを判定する判定手段と、

40

前記判定手段の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データの起動を終了する終了手段と、

前記判定手段の判定の結果、前記アプリケーションの起動が成功した場合は、

前記電子情報を復元し該アプリケーションからの操作が可能な状態にする操作手段と、

前記復元した電子情報を前記起動したアプリケーションに渡す処理手段とを備えることを特徴とする情報処理装置。

【請求項 46】 前記制限属性情報に前記対象アプリケーションを特定するアプリケーション情報が含まれない

50

場合、前記アプリケーション起動手段は起動すべきアプリケーションを自動認識することを特徴とする請求項 45 に記載の情報処理装置。

【請求項 47】 前記起動したアプリケーションが前記復元した電子情報を解放した場合に、該復元した電子情報を抹消する第 1 抹消手段と、

前記起動したアプリケーションが終了した場合に、前記起動した制限ルーチン部を終了し、抹消する第 2 抹消手段とを備えることを特徴とする請求項 45 に記載の情報処理装置。

【請求項 48】 電子情報を変換して操作を制限する情報処理方法であって、

電子情報を読み込み記憶媒体に記憶する記憶工程と、前記電子情報に対する操作を制限する内容を定義した制限属性情報を、該電子情報に付加する第 1 付加工程と、前記電子情報に対する操作を監視し制御する制限プログラムを、該電子情報に付加する第 2 付加工程と、前記第 1 及び第 2 付加工程によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力工程とを備えることを特徴とする情報処理方法。

【請求項 49】 実行可能形式データを利用する情報処理方法であって、

実行可能形式データを起動する起動工程と、前記制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込工程と、

前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得工程と、

前記取得工程で取得したアプリケーションを起動するアプリケーション起動工程と、

前記アプリケーション起動工程によるアプリケーションの起動が成功したかどうかを判定する判定工程と、

前記判定工程の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データの起動を終了する終了工程と、

前記判定工程の判定の結果、前記アプリケーションの起動が成功した場合は、元の電子情報を復元し該アプリケーションからの操作が可能な状態にする操作工程と、前記復元した電子情報を前記起動したアプリケーションに渡す処理工程とを備えることを特徴とする情報処理方法。

【請求項 50】 前記制限属性情報に前記対象アプリケーションを特定するアプリケーション情報が含まれない場合、前記アプリケーション起動工程は、起動すべきアプリケーションを自動認識することを特徴とする請求項 49 に記載の情報処理方法。

【請求項 51】 前記起動したアプリケーションが前記復元した電子情報を解放した場合に、該復元した電子情報を抹消する第 1 抹消工程と、

前記起動したアプリケーションが終了した場合に、前記起動した制限ルーチン部を終了し、抹消する第 2 抹消工程とを備えることを特徴とする請求項 49 に記載の情報処理方法。

【請求項 52】 第 1 端末と第 2 端末とが通信網を介して相互に接続されて構成される情報処理システムであって、

前記第 1 端末は、

電子情報を読み込み記憶する記憶手段と、

10 前記電子情報に対する操作を制限する内容を定義した制限属性情報を、前記該電子情報に付加する第 1 付加手段と、

前記電子情報に対する操作を監視し制御する制限プログラムを前記該電子情報に付加する第 2 付加手段と、

前記第 1 及び第 2 付加手段によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力手段と、

前記実行可能形式データを、前記第 2 端末に送信する送信手段とを備え、

20 前記第 2 端末は、前記実行可能形式データを、前記第 1 端末より受信する受信手段と、

前記実行可能形式データを起動する起動手段と、

前記制限プログラムから前記電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込手段と、

前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得手段と、

前記取得手段で取得したアプリケーションを起動するアプリケーション起動手段と、

30 前記アプリケーション起動手段によるアプリケーションの起動が成功したかどうかを判定する判定手段と、

前記判定手段の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データの起動を終了する終了手段と、

前記判定手段の判定の結果、前記アプリケーションの起動が成功した場合は、前記電子情報を復元し該アプリケーションからの操作が可能な状態にする操作手段と、

前記復元した電子情報を前記起動したアプリケーションに渡す処理手段とを備えることを特徴とする情報処理装置システム。

【請求項 53】 電子情報を変換して操作を制限する情報処理をコンピュータに機能させるためのプログラムであって、

電子情報を読み込み記憶する記憶工程のプログラムコードと、

前記電子情報に対する操作を制限する内容を定義した制限属性情報を、該電子情報に付加する第 1 付加工程のプログラムコードと、

50 前記電子情報に対する操作を監視し制御する制限プログラムを、該電子情報に付加する第 2 付加工程のプログラ

ムコードと、
前記第1及び第2付加工程によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力工程のプログラムコードとを備えることを特徴とするプログラム。

【請求項54】 実行可能形式データを利用する情報処理をコンピュータに機能させるためのプログラムであって、

電子情報に対する操作を制限する内容を定義した制限属性情報及び電子情報に対する操作を監視し制御する制限プログラムが付加された電子情報を含む実行可能形式データを起動する起動工程のプログラムコードと、

前記制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込工程のプログラムコードと、

前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得工程のプログラムコードと、

前記取得工程で取得したアプリケーションを起動するアプリケーション起動工程のプログラムコードと、

前記アプリケーション起動工程によるアプリケーションの起動が成功したかどうかを判定する判定工程のプログラムコードと、

前記判定工程の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データを終了する終了工程のプログラムコードと、

前記判定工程の判定の結果、前記アプリケーションの起動が成功した場合は、前記電子情報を復元し該アプリケーションからの操作が可能な状態にする操作工程のプログラムコードと、

前記復元した電子情報を前記起動したアプリケーションに渡す処理工程のプログラムコードとを備えることを特徴とするプログラム。

【請求項55】 前記制限属性情報に前記対象アプリケーションを特定するアプリケーション情報が含まれない場合、前記アプリケーション起動工程は、起動すべきアプリケーションを自動認識することを特徴とする請求項54に記載のプログラム。

【請求項56】 前記起動したアプリケーションが、前記復元した電子情報を解放した場合に、該復元した電子情報を抹消する第1抹消工程のプログラムコードと、前記起動したアプリケーションが終了した場合に、前記起動した制限ルーチンを終了し、抹消する第2抹消工程のプログラムコードとを備えることを特徴とする請求項54に記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ファイル、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを管理するコンピュータリソースの制

御方法および装置並びに記憶媒体に関するものである。

【0002】

【従来の技術】従来において、パーソナルコンピュータ等のコンピュータにおけるファイルや記憶装置等のリソースにアプリケーションプログラムを介してユーザがアクセスする場合に、アクセス権限のないユーザに情報が解読または盗聴されるのを防ぐために、オペレーティングシステム（以下、OS）内にアクセス権限のチェック機能を設ける方法、あるいは専用のアクセス管理ツールを付加してアクセス権限のチェックを行なう方法が知られている。

【0003】例えばWindows（米国マイクロソフト社の登録商標）に代表される汎用のOSにおいては、ファイルの読み取り、書き込み、実行をアクセス権限のないユーザに対しては許可しない機能が備わっている。また、ファイルの削除、アクセス権限の変更、所有権の変更についての権限を設定可能にした汎用OSもある。

【0004】また、アクセス管理ツールとして、例えば特開平7-84852公報に開示されているように、ファイルの参照と共に複写の可否を登録し、その可否によって参照、複写を制限するものが知られている。詳しくは、表示領域に読み出し制限の属性を付加し、表示画面のキャプチャーを防止するものが知られている。

【0005】

【発明が解決しようとする課題】アクセス権限のないユーザに対して情報の持ち出しを全面的に禁止するためには、図9に示すように、メールへの添付、印刷、ファイル移動／ファイルコピー、クリップボードへのコピー、フレキシブルディスクへの別名保存、オブジェクトの貼り付け、画面のキャプチャーなどの機能を制限する必要がある。さらに、ネットワークを通じた情報の持ち出しを制限する必要がある。

【0006】しかしながら、上記従来技術にあっては、ファイル移動／ファイルコピー及び画面のキャプチャー以外の操作（例えばクリップボードへのコピー）に対して制限することができないという問題がある。もしも、クリップボードへのコピーなどの操作を制限しようとする場合には、OSまたはアプリケーション自体に変更を加えることが必要になり、汎用的な応用ができないという問題がある。

【0007】本発明の目的は、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張することができるコンピュータリソースの制御が可能な情報処理装置及びその方法、記憶媒体を提供することにある。

【0008】

【課題を解決するための手段】上記の目的を達成するた

めの本発明による情報処理方法は以下の構成を備える。即ち、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理方法であって、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程と、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程とを備える。また、好ましくは、前記捕捉工程は、更に、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する。

【0009】また、好ましくは、前記判定工程は、特定のコンピュータリソースを指定するリソース指定情報、アクセス権限が有効となる条件情報、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を含むアクセス権限管理テーブルを参照して、アクセス権限があるか否かを判定する。

【0010】また、好ましくは、前記判定工程は、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を参照して、アクセス権限があるか否かを判定する。

【0011】また、好ましくは、前記判定工程は、アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定する。

【0012】また、好ましくは、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面キャプチャ権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含む。

【0013】また、好ましくは、前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す。

【0014】また、好ましくは、前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す。

【0015】また、好ましくは、前記拒否工程は、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す。

【0016】上記の目的を達成するための本発明による情報処理装置は以下の構成を備える。即ち、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等の

オペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理装置であって、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉手段と、前記捕捉手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定手段と、前記判定手段の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理手段と、前記判定手段の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否手段とを備える。

【0017】上記の目的を達成するための本発明による記憶媒体は以下の構成を備える。即ち、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するプログラムコードを記憶した記憶媒体であって、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備える。

【0018】上記の目的を達成するための本発明によるプログラムは以下の構成を備える。即ち、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスの制御をコンピュータに機能させるためのプログラムであって、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備える。

【0019】上記の目的を達成するための本発明による情報処理システムは以下の構成を備える。即ち、前記第1端末は、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作

要求をコンピュータリソースにアクセスする前に捕捉する捕捉手段とを備え、前記第2端末は、前記捕捉手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定手段と、前記判定手段の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理手段と、前記判定手段の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否手段とを備える。

【0020】上記の目的を達成するための本発明による情報処理システムの制御方法は以下の構成を備える。即ち、第1端末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムの制御方法であって、前記第1端末において、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程と、前記第2端末において、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程とを備える。

【0021】上記の目的を達成するための本発明による記憶媒体は以下の構成を備える。即ち、第1端末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムの制御のプログラムコードを記憶した記憶媒体であって、前記第1端末において、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、前記第2端末において、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備える。

【0022】上記の目的を達成するための本発明によるプログラムは以下の構成を備える。即ち、第1端末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムの制御をコンピュータに機能させるためのプログラムであって、前記第1端末において、前記第2端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプ

ログラムコードと、前記第2端末において、前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記第1端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備える。

【0023】上記の目的を達成するための本発明による情報処理装置は以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置であって、前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉手段と、前記操作要求に対する回答を受信する受信手段とを備える。

【0024】上記の目的を達成するための本発明による情報処理装置は以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置であって、当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定手段と、前記判定手段の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理手段と、前記判定手段の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否手段とを備える。

【0025】上記の目的を達成するための本発明による情報処理方法は以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置の情報処理方法であって、前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程と、前記操作要求に対する回答を受信する受信工程とを備える。

【0026】上記の目的を達成するための本発明による情報処理方法は以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置の情報処理方法であって、当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、前記判定工程の判定の結

果、アクセス権限がなければ当該操作要求を拒否する拒否工程とを備える。

【0027】上記の目的を達成するための本発明による記憶媒体は以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置の情報処理のプログラムコードを記憶した記憶媒体であって、前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、前記操作要求に対する回答を受信する受信工程のプログラムコードとを備える。

【0028】上記の目的を達成するための本発明による記憶媒体は以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置の情報処理のプログラムコードを記憶した記憶媒体であって、当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備える。

【0029】上記の目的を達成するための本発明によるプログラムは以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置の情報処理をコンピュータに機能させるためのプログラムであって、前記他の端末のコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する捕捉工程のプログラムコードと、前記操作要求に対する回答を受信する受信工程のプログラムコードとを備える。

【0030】上記の目的を達成するための本発明によるプログラムは以下の構成を備える。即ち、通信網を介して他の端末と接続する情報処理装置の情報処理をコンピュータに機能させるためのプログラムであって、当該情報処理装置のコンピュータリソースにアクセスする前に、前記他の端末で捕捉された前記コンピュータリソースに対する操作要求によって指定される該コンピュータリソースに対するアクセス権限があるか否かを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りに前記他の端末のオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程のプログラムコードと、前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程のプログラムコードとを備える。

【0031】上記の目的を達成するための本発明による

情報処理装置は以下の構成を備える。即ち、電子情報提供側の情報処理装置においては、電子情報に対する操作を制限するよう電子情報をプロテクション化する情報処理装置であって、対象の電子情報にアクセス可能なコンピュータと、対象の電子情報およびプロテクション化電子情報を格納するメモリもしくはハードディスクなどの記憶媒体と、電子情報を提供するための手段としてフレキシブルディスクドライブなどの外部メディア装置もしくは通信回線等を備える。一方、電子情報受け取り側の情報処理装置においては、プロテクション化電子情報を利用する情報処理装置であって、受け取ったプロテクション化電子情報にアクセス可能であり対象の電子情報が利用可能なコンピュータと、プロテクション化電子情報および対象の電子情報を一時的に格納するメモリもしくはハードディスクなどの記憶媒体と、電子情報の利用内容に応じてディスプレイ、プリンタ、キーボード等の入出力装置と、プロテクション化電子情報を受け取るための手段としてフレキシブルディスクドライブなどの外部メディア装置もしくは通信回線等を備える。

【0032】ここで、プロテクション化電子情報とは、対象の電子情報に対する操作を制御する制限プログラムと、電子情報に対して印刷禁止や複製禁止といった制限する操作の内容を定義した制限属性を、対象の電子情報に付加し、実行可能形式にしたものである。

【0033】対象の電子情報に対して制限プログラムと制限属性を付加することで元の電子情報を変換する処理をプロテクション化と呼び、プロテクション化した電子情報をプロテクション化電子情報と呼ぶことにする。また、プロテクション化を実現するプログラムをプロテクション化プログラムと呼ぶことにする。

【0034】また、制限プログラムは、プロテクション化電子情報を元の電子情報として利用可能にするための展開ルーチン部と、電子情報へのアクセスを制御するための制限ルーチン部からなる。

【0035】さらに、制限属性は、電子情報に対して制限する操作と条件の組を1組以上保持し、必要に応じて、電子情報にアクセスするためのアプリケーション等のプログラムを特定する情報を保持する。

【0036】ここで、アプリケーションとは、電子情報にアクセスするために使用されるプログラムを指し、例えば、文書ファイルにアクセスするためのワープロソフトや、画像や動画を再生または編集するプログラムなどがそれに相当する。

【0037】アプリケーションはユーザが必ずしも操作するものとは限らず、一般的にOSもしくはプラットフォームの機能を利用して電子情報にアクセスするプログラムを、総称してここではアプリケーションと呼ぶことにする。

【0038】また、OS（オペレーティングシステム）にはマイクロソフト社のWindowsやアップル社の

10

20

30

40

50

Mac OS、さらに一般的にUNIX (X/Open社の登録商標)と呼ばれるものがあり、携帯端末機などでもOSは稼動している。さらに、ここでいうプラットフォームとは、OSのことを指すこともあるが、より広く、Web情報を閲覧するブラウザソフトなども、電子情報を扱う汎用的な環境を提供し、その上で実行可能な形式のプログラムを実行することができるコンピュータ上の基本プログラムという意味で、プラットフォームに含めることにする。

【0039】本発明の電子情報を提供する側の情報処理装置には電子情報を読み込み記憶する記憶手段と、前記電子情報に対する操作を制限する内容を定義した制限属性情報を、前記該電子情報に付加する第1付加手段と、前記電子情報に対する操作を監視し制御する制限プログラムを、前記該電子情報に付加する第2付加手段と、前記第1及び第2付加手段によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力手段とを備える。

【0040】また、本発明の電子情報を受け取る側の情報処理装置ではプロテクション化電子情報の実行が可能であり、プロテクション化電子情報を実行した際の処理は、電子情報に対する操作を制限する内容を定義した制限属性情報及び電子情報に対する操作を監視し制御する制限プログラムが付加された電子情報を含む実行可能形式データを起動する起動手段と、前記制限プログラムから前記電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込手段と、前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得手段と、前記取得手段で取得したアプリケーションを起動するアプリケーション起動手段と、前記アプリケーション起動手段によるアプリケーションの起動が成功したかどうかを判定する判定手段と、前記判定手段の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データの起動を終了する終了手段と、前記判定手段の判定の結果、前記アプリケーションの起動が成功した場合は、前記電子情報を復元し該アプリケーションからの操作が可能な状態にする操作手段と、前記復元した電子情報を前記起動したアプリケーションに渡す処理手段とを備える。

【0041】また、好ましくは、前記制限属性情報に前記対象アプリケーションを特定するアプリケーション情報が含まれない場合、前記アプリケーション起動手段は起動すべきアプリケーションを自動認識する。

【0042】自動認識の例としては、電子情報がファイルである場合にはその拡張子からアプリケーションがOSによって定義されている場合があり、それを利用するケースがある。また、電子情報を受け取る側の環境によってはアプリケーションが特定できる場合がある。このように電子情報を利用する際に使用するアプリケーションが自明である場合には、前記第1付加手段における制

限属性内にアプリケーション情報は必要ではなく、前記アプリケーション起動手段において起動すべきアプリケーションの自動認識が可能となる。

【0043】また、好ましくは、前記起動したアプリケーションが前記復元した電子情報を解放した場合に、該復元した電子情報を抹消する第1抹消手段と、前記起動したアプリケーションが終了した場合に、前記起動した制限ルーチン部を終了し、抹消する第2抹消手段とを備える。

【0044】上記の目的を達成するための本発明による情報処理方法は以下の構成を備える。即ち、電子情報を提供する側においては、電子情報をプロテクション化する情報処理方法であって、電子情報を読み込み記憶媒体に記憶する記憶工程と、前記電子情報に対する操作を制限する内容を定義した制限属性情報を、該電子情報に付加する第1付加工程と、前記電子情報に対する操作を監視し制御する制限プログラムを、該電子情報に付加する第2付加工程と、前記第1及び第2付加工程によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力工程とを備える。また、電子情報を受け取る側においては、プロテクション化電子情報(実行可能形式データ)を利用するための情報処理方法であって、実行可能形式データを起動する起動工程と、前記制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込工程と、前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得工程と、前記取得工程で取得したアプリケーションを起動するアプリケーション起動工程と、前記アプリケーション起動工程によるアプリケーションの起動が成功したかどうかを判定する判定工程と、前記判定工程の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データの起動を終了する終了工程と、前記判定工程の判定の結果、前記アプリケーションの起動が成功した場合は、元の電子情報を復元し該アプリケーションからの操作が可能な状態にする操作工程と、前記復元した電子情報を前記起動したアプリケーションに渡す処理工程とを備える。

【0045】また、好ましくは、前記制限属性情報に前記対象アプリケーションを特定するアプリケーション情報が含まれない場合、前記アプリケーション起動工程は、起動すべきアプリケーションを自動認識する。

【0046】また、好ましくは、前記起動したアプリケーションが前記復元した電子情報を解放した場合に、該復元した電子情報を抹消する第1抹消工程と、前記起動したアプリケーションが終了した場合に、前記起動した制限ルーチン部を終了し、抹消する第2抹消工程とを備える。

【0047】上記の目的を達成するための本発明による情報処理システムは以下の構成を備える。即ち、第1端

末と第2端末とが通信網を介して相互に接続されて構成される情報処理システムであって、前記第1端末は、電子情報を読み込み記憶する記憶手段と、前記電子情報に対する操作を制限する内容を定義した制限属性情報を、前記該電子情報に付加する第1付加手段と、前記電子情報に対する操作を監視し制御する制限プログラムを前記該電子情報に付加する第2付加手段と、前記第1及び第2付加手段によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力手段と、前記実行可能形式データを、前記第2端末に送信する送信手段とを備え、前記第2端末は、前記実行可能形式データを、前記第1端末より受信する受信手段と、前記実行可能形式データを起動する起動手段と、前記制限プログラムから前記電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込手段と、前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得手段と、前記取得手段で取得したアプリケーションを起動するアプリケーション起動手段と、前記アプリケーション起動手段によるアプリケーションの起動が成功したかどうかを判定する判定手段と、前記判定手段の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データの起動を終了する終了手段と、前記判定手段の判定の結果、前記アプリケーションの起動が成功した場合は、前記電子情報を復元し該アプリケーションからの操作が可能な状態にする操作手段と、前記復元した電子情報を前記起動したアプリケーションに渡す処理手段とを備える。

【0048】上記目的を達成するための本発明によるプログラムは以下の構成を備える。すなわち、電子情報提供側においては、電子情報に対する操作を制限するよう電子情報をプロテクション化するプログラムであって、電子情報を読み込み記憶する記憶工程のプログラムコードと、前記電子情報に対する操作を制限する内容を定義した制限属性情報を、該電子情報に付加する第1付加工程のプログラムコードと、前記電子情報に対する操作を監視し制御する制限プログラムを、該電子情報に付加する第2付加工程のプログラムコードと、前記第1及び第2付加工程によって前記制限属性情報及び前記制限プログラムが付加された前記電子情報をまとめて実行可能形式データで出力する出力工程のプログラムコードとを備える。

【0049】また、電子情報を受け取る側においては、プロテクション化電子情報を利用するためのプログラムであって、実行可能形式データを利用する情報処理をコンピュータに機能させるためのプログラムであって、電子情報に対する操作を制限する内容を定義した制限属性情報及び電子情報に対する操作を監視し制御する制限プログラムが付加された電子情報を含む実行可能形式データを起動する起動工程のプログラムコードと、前記制限

プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する読込工程のプログラムコードと、前記制限属性情報から前記電子情報を操作するための対象アプリケーションを取得する取得工程のプログラムコードと、前記取得工程で取得したアプリケーションを起動するアプリケーション起動工程のプログラムコードと、前記アプリケーション起動工程によるアプリケーションの起動が成功したかどうかを判定する判定工程のプログラムコードと、前記判定工程の判定の結果、前記アプリケーションの起動が失敗した場合は、前記実行可能形式データを終了する終了工程のプログラムコードと、前記判定工程の判定の結果、前記アプリケーションの起動が成功した場合は、前記電子情報を復元し該アプリケーションからの操作が可能な状態にする操作工程のプログラムコードと、前記復元した電子情報を前記起動したアプリケーションに渡す処理工程のプログラムコードとを備える。

【0050】また、好ましくは、前記制限属性情報に前記対象アプリケーションを特定するアプリケーション情報が含まれない場合、前記アプリケーション起動工程は、起動すべきアプリケーションを自動認識する。

【0051】また、好ましくは、前記起動したアプリケーションが前記復元した電子情報を解放した場合に、該復元した電子情報を抹消する第1抹消工程のプログラムコードと、前記起動したアプリケーションが終了した場合に、前記起動した制限ルーチンを終了し、抹消する第2抹消工程のプログラムコードとを備える。

【発明の実施の形態】

【第1実施形態】以下、本発明の実施の形態を図面により詳細に説明する。

【0052】図1(A)、(B)は本発明を実施する環境の一実施の形態を示すハードウェア構成図である。

【0053】図1(A)に示す構成は、スタンドアロン構成におけるコンピュータ101のハード構成を示すものであり、ハードディスクドライブ(HDD)1011を備えたパーソナルコンピュータ(PC)1012、ディスプレイ1013、プリンタ1014、外部にリソースデータを出力することが可能な外部装置1015で構成されている。

【0054】パーソナルコンピュータ1012には、汎用のOSとアプリケーションが組み込まれており、さらに本発明に係るリソース管理プログラムが組み込まれている。

【0055】図1(B)は、ネットワーク102を利用する場合の構成を示すものであり、図1(A)に示したのと同様な構成のコンピュータ101a~101cがネットワーク102を介して相互に接続されている。

【0056】このような構成において、一般的に、アプリケーションがOSの管理するリソースにアクセスするには、OSが提供するAPI(Application

10

20

30

40

50

Program Interface)を利用する。このAPIの利用方法はOSにより確定しており、APIを利用する実行コード部を判別することができる。本発明では、リソースへのアクセスに必要なすべてのAPIを監視する監視ルーチンを設け、アプリケーションがAPIを利用する前に、その実行コード部を変更するか、API処理の入りを監視ルーチンと置き換えることで、API利用時に監視ルーチンが利用されるようにする。監視ルーチンは、アプリケーションが求めるAPIを処理するか、もしくはAPIの処理をせず不正命令としてアプリケーションに結果を返す。本発明のリソース管理プログラムによって拡張したアクセス権限の管理は、OSの管理とは別に本プログラムが管理し、アクセス権限の種類別に監視ルーチンを設ける。この方法により、リソースを不正に利用するアプリケーションから、そのアクセスを制限する。

【0057】図2は、本発明に係るリソース管理プログラム203の構成及びAPI監視/制御の概念を示す図であり、リソース管理プログラム203はAPI監視コントローラ(API監視CTRL)2031、APL(アプリケーション)監視コントローラ(APL監視CTRL)2032、アクセス制御コントローラ(アクセス制御CTRL)2033、OS監視コントローラ(OS監視CTRL)2034から構成されている。このリソース管理プログラム203は、リソースアクセス要求を出すアプリケーション2021や画面キャプチャなどのOS機能操作2022を備える一般的なアプリケーションからなるユーザ環境202と汎用OS201との間に位置し、汎用OS201およびユーザ環境202が提供するリソースに対する要求を監視するようになって

いる。【0058】なお、汎用OS201は、OSが管理するリソース2011と、OSがアプリケーション2021に提供しているAPI群2012を備える。

【0059】本発明に係るリソース管理プログラム203におけるAPI監視CTRL2031は、アクセス制御を行なうのに必要な全てのAPIを監視するモジュールである。また、APL監視CTRL2032は、アプリケーション2021が保持しているリソースを記憶するモジュールである。アクセス制御CTRL2033はリソース2011のアクセスが許可されているかを判断するモジュールであり、アクセス権限管理テーブル2035を備える。また、OS監視CTRL2034は、汎用OS201の機能によってリソースへアクセスする操作を監視するモジュールである。

【0060】アクセス権限管理テーブル2035は、図3に示すように、リソース指定情報20351、条件20352、n個のアクセス権限情報20353~2035nをリソース毎に登録可能に構成されている。

【0061】リソース指定情報20351は、汎用OS

201が管理しているリソース2011のうち、特定のものを指定するための情報であり、例えば、ファイルの場合はファイル名やファイルIDなどの情報が登録される。通信データの場合は、ホスト名、ポート番号、IPアドレスなどが登録され、メモリの場合は、そのオブジェクトを示すオブジェクト名、アドレスなどが登録される。また、外部装置の場合は、そのデバイスドライバを示すデバイス名などが登録される。

【0062】条件20352は、アクセス権限が有効となる条件またはその組み合わせをしめすものであり、例えばユーザ名/ID、グループ名/ID、時刻、使用アプリケーションなどが登録される。

【0063】アクセス権限情報20353~2035nは、既存環境で定義されていない拡張したアクセス権限のうち、指定したリソースに付加した権限を示すものであり、例えば他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限(Windowsではクリップボードなど)、画面キャプチャ権限、使用アプリケーションの限定(特定アプリケーション以外での使用禁止やメール添付の禁止)などが登録される。

【0064】なお、一般的に、リソースへのアクセスは複数のAPIによって行われることがあり、その場合はリソース指定情報はOSが管理するID(ハンドルなど)に変換されることがある。その場合、リソース管理プログラム203の内部においては、リソース指定情報とそのIDは同一視するようにしている。

【0065】このような構成に係るリソース管理プログラム203の処理について、図2の①~④で示す情報伝達手順に従って説明する。

【0066】①アプリケーション2021が発行したAPIによってリソースへのアクセス要求があれば、API監視CTRL2031がその要求を捕捉し、アクセス制御CTRL2033に伝える。

【0067】②アクセス制御CTRL2033は、アクセス権限チェックを行なう際、必要に応じて、アプリケーション2021が保持しているリソースの情報をAPL監視CTRL2032から取得する。

【0068】③アクセスを拒否する条件として2通りあるが、第1の条件A(アクセス拒否A)では、上記①のアクセス要求に対して、アクセス権限管理テーブル2035を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がない場合、アプリケーション2021が発行したAPIの処理を行わずに、結果としてアクセス違反のエラーを返す。

【0069】④第2の条件B(アクセス拒否B)では、①のアクセス要求に対して、アクセス権限管理テーブル2035を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がなく、かつ、アプリケーション2021が発行したAPI{処理}の結果

としてエラーを返すことができない場合、アプリケーション2021が要求したリソースへの処理を行なわずに、リソース管理プログラム203が予め用意したダミーのリソースへのアクセス要求に代えて、APIの処理を行なう。

【0070】その結果、アプリケーション2021は要求に成功したように動作するが、実際には要求したリソースにアクセスできない。

【0071】⑤アクセス要求⑤に対してアクセス権限チェックを行った結果、権限がある場合、API監視CTRL2031がそのアクセス要求を捕捉し、アプリケーション2021が発行したAPIの処理をそのまま汎用OS201に伝え、その結果をアプリケーション2021に返す。

【0072】⑥上記⑤の処理によって、APIが成功し、かつ、そのAPIによってアプリケーション2021がリソースを保持する場合は、APL監視CTRL2032に伝える。APL監視CTRL2032はアプリケーション2021と保持しているリソースの対応を登録する。

【0073】アプリケーション2021がリソースの解放要求APIを発行し、かつそのAPIが成功した場合も、APL監視CTRL2032に伝える。APL監視CTRL2032はアプリケーション2021と保持していたリソースの対応を抹消する。

【0074】⑦OS標準機能の操作によって、リソースへのアクセス要求があれば、OS監視CTRL2034がそのアクセス要求を捕捉し、アクセス制御CTRL2033に伝える。

【0075】⑧アクセス要求⑦に対して、アクセス権限管理テーブル2035を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がない場合、⑦の操作を無視する。

【0076】⑨アクセス要求⑦に対して、アクセス権限管理テーブル2035を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がある場合、⑦の操作を汎用OS201に伝える。

【0077】図4は、目的とするリソースに対するアクセス権限がある場合に、そのリソースを解放するまでのアプリケーション2021、リソース管理プログラム203、汎用OS201のやり取りを示したAPIの監視及び制御の第1の基本型(1)のシーケンス図である。

【0078】この第1の基本型(1)では、アプリケーション2021が発行したAPIによって目的のリソースへのアクセス要求があった場合(ステップ401)、リソース管理プログラム203はアプリケーション2021がそのリソースへのアクセス権限があるかをチェックする(ステップ402)。チェックの結果、アクセス権限がある場合(ステップ403)、汎用OS201にアプリケーション2021が発行したAPIをそのまま

伝える。汎用OS201は、OS本来のAPI処理を行なう(ステップ404)。

【0079】リソース管理プログラム203は、API処理が成功した場合、アプリケーション2021がそのリソースを保持しているという情報を登録する(ステップ405)。そして、汎用OS201からのAPI結果をそのままアプリケーション2021に返す(ステップ406)。これにより、リソースへのアクセス完了となる(ステップ407)。

【0080】この後、アプリケーション2021から保持しているリソースの解放要求が発行された場合(ステップ408)、リソース管理プログラム203はその解放要求を汎用OS201に伝える。汎用OS201は、OS本来のAPI処理を行なう(ステップ409)。リソース管理プログラム203は、API処理が成功した場合、アプリケーション2021がそのリソースを保持しているという情報を解除する(ステップ410)。そして、汎用OS201からのAPI結果をそのままアプリケーション2021へ返す(ステップ411)。これにより、保持しているリソースの解放完了となる(ステップ412)。

【0081】図5は、目的とするリソースに対するアクセス権限がなかった場合に、そのアクセスが拒否されるまでのアプリケーション2021、リソース管理プログラム203、汎用OS201のやり取りを示したAPIの監視及び制御の第2の基本型(2)のシーケンス図である。

【0082】この第2の基本型(2)では、アプリケーション2021が発行したAPIによって目的のリソースへのアクセス要求があった場合(ステップ501)、リソース管理プログラム203はアプリケーション2021がそのリソースへのアクセス権限があるかをチェックする(ステップ502)。チェックの結果、アクセス権限がなかった場合(ステップ503)、アクセス違反エラーをアプリケーション2021に返す(ステップ504)。これにより、リソースへのアクセス処理終了となる(ステップ505)。

【0083】また、アクセス違反エラーに対応していないアプリケーション2021が発行したAPIによって目的のリソースへのアクセス要求があった場合(ステップ506)、リソース管理プログラム203はアプリケーション2021がそのリソースへのアクセス権限があるかをチェックする(ステップ507)。チェックの結果、アクセス権限がなく、かつ、アプリケーション2021がアクセス違反エラーに対応していない場合(ステップ508)、リソース管理プログラム203が予め用意したダミーのリソースへのアクセス要求に置き換え、汎用OS201に渡す(ステップ509)。

【0084】汎用OS201は、OS本来のAPI処理を行なう(ステップ510)。リソース管理プログラム

203は、汎用OS201からのAPI処理結果をそのままアプリケーション2021へ返す(ステップ511)。この結果、目的のリソースへのアクセス処理終了となるが、ダミーリソースのため、実質的には何も行われない(ステップ512)。

【0085】本発明は、以上のようにしてアクセス権のないリソースへのアクセスを制限するものであるが、汎用のOSであるWindowsとUNIXの場合のAPIを例に挙げて説明する。

【0086】まず、ファイルへの複製処理を禁止する例について説明する。

【0087】ファイルへの複製処理については、従来、読み込み許可ファイルはファイルのコピーが可能であり、その結果オリジナルの複製が複数存在したり、別媒体に転写して持ち出すことが可能であった。本発明では、ファイルコピーを実現するAPIを監視/制御することにより、権限のないファイルのコピーを禁止する。その場合に、Windowsにおいて監視/制御するAPIとして次のものがある。なお、以下で例示するAPIの機能については、各種の文献で公開されているので、その詳細な説明は省略する。

【0088】(1) ファイルオープン/作成API

```
CreateFileA
CreateFileW
OpenFile
_lopen
_lcreat
GetOpenFileNameA
GetOpenFileNameW
GetSaveFileNameA
GetSaveFileNameW
```

(2) ファイルクローズAPI

```
CloseHandle
_lclose
```

(3) ファイルコピー/移動API

```
CopyFileA
CopyFileW
MoveFileA
MoveFileW
MoveFileExA
MoveFileExW
DeleteFileA
DeleteFileW
DragQueryFileA
DragQueryFileW
```

UNIXの場合、監視/制御するAPIとしては次のものがある。

【0089】(1) ファイルオープン/作成API

```
open
creat
```

(2) ファイルクローズAPI

```
close
```

(3) ファイルコピー/移動API

```
rename
```

このようなAPIの監視によってファイルへの複製処理を禁止する場合、具体的な方法として3つの方法がある。

【0090】<方法1>(ファイルオープン中に複製処理を行なうことが判明している場合)

アプリケーションが、複製権限のないファイルをオープンし保持している間(ファイルをクローズするまでの期間)、そのアプリケーションが別のファイルを作成することを拒否する。

【0091】<方法2>(ファイルクローズ後に複製処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合)

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複製権限のあるファイルをオープンするまで、そのアプリケーションが別のファイルを作成することを拒否する。

【0092】<方法3>(ファイルクローズ後に複製処理を行なう可能性があり、複数ファイルを扱う可能性がある場合)

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが別のファイルを作成することを拒否する。

【0093】なお、いずれの方法であっても、別に作成されるファイルによって複製が残ることがないと判明している場合(一時ファイルなどの作成)は拒否しない。

【0094】次に、特定ファイルまたは全ての印刷を禁止する例について説明する。

【0095】従来、印刷機能を実装したアプリケーションによって、ファイルの内容を印刷し、外部に持ち出すことは可能であった。本発明では、印刷を実現するAPIを監視/制御することにより、印刷権限のないファイルの印刷を禁止する。また、FAXなどその他の外部装置についても、それぞれの外部装置の選択や制御を実現するAPIを監視/制御することにより、同様に禁止する。その場合に、Windows及びUNIXにおいて監視/制御するAPIとして次のものがある。

【0096】Windowsの場合

(1) デバイスオープンAPI

```
CreateDCA
```

```
CreateDCW
```

(2) デバイスクローズAPI

```
ReleaseDC
```

```
ClosePrinter
```

(3) プリンタ選択/APL処理API

OpenPrinterA
 OpenPrinterW
 GetPrinterA
 GetPrinterW
 SetPrinterA
 SetPrinterW
 SendMessageA
 SendMessageW
 PostMessageA
 PostMessageW
 UNIXの場合
 (1) デバイスオープンAPI
 open
 (2) デバイス制御API
 ioctl
 (3) デバイスクローズAPI
 close

このようなAPIの監視によって印刷処理を禁止する場合、具体的な方法として3つの方法がある。

【0097】<方法1>（ファイルオープン中に印刷処理可能なことが判明している場合）

アプリケーションが、印刷権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンに拒否する。

【0098】<方法2>（ファイルクローズ後に印刷処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、印刷権限のあるファイルをオープンするまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンに拒否する。

【0099】<方法3>（ファイルクローズ後に印刷処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンに拒否する。

【0100】次に、外部装置の利用を禁止する例について説明する。

【0101】従来、OSに装備されている機能や外部装置そのものに権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきAPIを限定できる機能の指定や、外部装置利用の指定をすることにより、その利用を禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

【0102】Windowsの場合

(1) デバイスオープンAPI
 CreateFileA
 CreateFileW
 OpenFile
 _lopen
 _lcreat
 (2) デバイスクローズAPI
 CloseHandle
 _lclose

10 UNIXの場合

(1) デバイスオープンAPI
 open
 (2) デバイス制御API
 ioctl
 (3) デバイスクローズAPI
 close

例えば、このようなAPIの監視によって印刷を禁止する場合、具体的な方法として次の方法がある。

【0103】<方法>アクセス権管理テーブル2035にて、特定の条件のもとに特定外部装置の使用を禁止されている場合、その外部装置の利用を以下の方法で拒否する。その外部装置のデバイス名をもってデバイスオープンAPI要求があった場合、アクセス禁止エラー、もしくは外部装置が存在しないというエラーを返すことで要求を拒否する。

【0104】次に、ファイル内の一部のデータまたは全ての複写を禁止する例について説明する。

【0105】従来、アプリケーションによってファイルを画面表示した結果、その内容のすべてまたは一部をOSの機能によって複写することまたはオブジェクトという単位で別ファイルに埋め込むことが可能であった。

【0106】本発明では、転写や埋め込み機能を実現するAPI（クリップボードのAPI、OLEのAPIなど）を監視／制御することで、複写権限のないデータの流用を禁止する。

【0107】その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

【0108】Windowsの場合

(1) 複写／埋め込みAPI
 40 OpenClipboard
 SetClipboardData
 GetClipboardData
 GetOpenClipboardWindow
 OleCreate
 OleCreateEx
 OleCreateFromFile
 OleCreateFromFileEx
 OleCreateFromData
 OleCreateFromDataEx
 50 OleCreateLink

OleCreateLinkEx
OleCreateLinkFromData
OleCreateLinkFromDataEx
OleCreateLinkToFile
OleCreateLinkToFileEx
CloseClipboard

このようなAPIの監視によって複写処理を禁止する場合、具体的な方法として4つの方法がある。

【0109】<方法1>（ファイルオープン中に複写処理可能なことが判明している場合）

アプリケーションが、複写権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

【0110】<方法2>（ファイルクローズ後に複写処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複写権限のあるファイルをオープンするまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

【0111】<方法3>（ファイルクローズ後に複写処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

【0112】<方法4>（複写権限のないファイルを埋め込みオブジェクトとして取り込む場合）

複写権限のないファイルを取り込む処理を行なう際に、オブジェクトの登録もしくはそのオブジェクトの取得APIにおいて、アクセス違反のエラーを返すか、空データを登録あるいは取得することで、処理要求を拒否する。

【0113】次に、ネットワークを介してファイルが外部へ流出することを禁止する例について説明する。

【0114】従来、ファイルコピー以外に、FTPプログラムのように、ネットワークを介してファイルを外部へ転送することは可能であった。本発明では、ネットワークリソースにアクセスするAPIを監視／制御することで、外部出力権限のないファイルを使用中のアプリケーションから、外部へのファイル内容の出力を禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

【0115】Windowsの場合

WSAStartup
accept
bind
connect
gethostbyname
gethostbyaddr
getprotobyname
getprotobynumber
getservbyname
getservbyport
getpeername
getsockname
gethostname
getsockopt
setsockopt
recv
recvfrom
socket
select
send
sendto
WSASend
WSASendTo
WSAAsyncSelect
WSAAsyncGetHostByAddr
WSAAsyncGetHostByName
WSAAsyncGetProtoByNumber
WSAAsyncGetProtoByName
WSAAsyncGetServByPort
WSAAsyncGetServByName
WSACancelAsyncRequest
WSASetBlockingHook
WSAUnhookBlockingHook
WSACleanup
closesocket
shutdown
UNIXの場合
accept
bind
connect
gethostbyname
gethostbyaddr
getprotobyname
getprotobynumber
getservbyname
getservbyport
getpeername
getsockname
gethostname
getsockopt

```

setsockopt
recv
recvfrom
socket
select
send
sendto
closesocket
shutdown

```

このようなAPIの監視によって使用中のアプリケーションから外部へのデータ出力を禁止する場合、具体的な方法として3つの方法がある。

【0116】＜方法1＞（ファイルオープン中に出力処理可能なことが判明している場合）

アプリケーションが、外部出力権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションからの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

【0117】＜方法2＞（ファイルクローズ後に出力処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、出力権限のあるファイルをオープンするまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

【0118】＜方法3＞（ファイルクローズ後に出力処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

【0119】ただし、その通信によってデータ出力されないことが判明している場合は、拒否しない。

【0120】次に、ファイルの内容のイメージを取得することを禁止する例について説明する。

【0121】OSの機能として画面全体や一部、またはウインドウ単位の画面をイメージデータとして取得することが、一般的には可能であり、従来、そのイメージデータを流用、持ち出すことができた。本発明では、画面内のイメージデータ取得APIを監視／制御することで、イメージデータ取得を禁止する。

【0122】その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

【0123】（1）デバイスオープンAPI

```

GetWindowDC
WindowFromDC

```

```

GetDC
GetDCEx
GetDesktopWindow
GetDeviceCaps
CreateDCA
CreateDCW

```

（2）イメージ取得API

```

BitBlt
StretchBlt

```

（3）デバイスクローズAPI

```

DeleteDC
ReleaseDC

```

このようなAPIの監視によって画面イメージを取得することを禁止する場合、具体的な方法として3つの方法がある。

【0124】＜方法1＞（画面全体のキャプチャーを拒否する場合）

現在画面上に表示されているウインドウを所有しているアプリケーションが、画面イメージ取得権限のないファイルを保持している場合、画面全体のイメージ取得を拒否する。画面全体のイメージ取得処理の有無は、画面全体を管理しているウインドウ（Windowsの場合はデスクトップウインドウ）の状態を監視することで行なう。WindowsにおけるDirectDrawなど、画面全体のイメージを取得するAPIが存在すれば、同様に拒否する。

【0125】さらに、ディスプレイデバイスからVRAMイメージを取得するアプリケーションに対しては、それを拒否する。

30 【0126】＜方法2＞（ウインドウの画面イメージ取得を拒否する場合）

現在画面上に表示されているウインドウを所有しているアプリケーションが、画面イメージ取得権限のないファイルを保持している場合、そのウインドウのイメージ取得を拒否する。ウインドウが画面上に表示されているかは、ウインドウの状態を監視することで行なう。

【0127】また、画面イメージ取得の拒否は、そのウインドウに関連付けられたデバイスコンテキストからのイメージコピーを拒否することで行なう。

40 【0128】＜方法3＞（画面の一部のイメージ取得を拒否する場合）

画面イメージを取得する領域が判断できる場合は、＜方法1＞における条件を、取得領域が対象となるウインドウと重なる時とし、以降は＜方法1＞と同様にして画面の一部のイメージ取得を拒否する。また、領域が判断できない時は、＜方法1＞と同様にして画面全体のイメージ取得を拒否する。

【0129】次に、ファイル種別毎に利用アプリケーションを限定する例について説明する。

50 【0130】従来、アプリケーション利用に制限がない

ため、参照以外の目的でファイルにアクセス可能であった。本発明では、ファイルごとに利用アプリケーションを限定できる。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

【0131】(1) ファイルオープンAPI

CreateFileA

CreateFileW

OpenFile

_lopen

_lcreat

(2) ファイルクローズAPI

CloseHandle

_lclose

(3) プロセス管理API

WinExec

CreateProcessA

CreateProcessW

ExitProcess

UNIXの場合

(1) ファイルオープンAPI

open

(2) ファイルクローズAPI

close

このようなAPIの監視によって利用アプリケーションを限定する場合、具体的な方法として次の方法がある。
＜方法＞アプリケーションがファイルをオープンする際、そのファイルの権限をチェックし、許可されたアプリケーションでない場合はアクセス違反エラーを返すことで、オープン要求を拒否する。

【0132】次に、OSに装備されている特定の機能の利用を禁止する例について説明する。

【0133】従来、OSに装備されている機能に権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきAPIを限定する機能を指定することで、その利用を禁止することができる。例えば、ファイルのタイムスタンプやシステム日時の変更を禁止するなどである。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

【0134】(1) ファイルのタイムスタンプ変更API

SetFileTime

(2) システム日時の変更API

SetSystemTime

SetSystemTimeAdjustment

このようなAPIの監視によってOSにおける特定の機能の利用を禁止する場合、具体的な方法として次の方法がある。

【0135】＜方法＞特定の条件下で禁止されているAPIが発行された際に、アクセス違反エラーを返すか、実際の処理を行わずにダミー処理を施し、正常リター

ンすることで、禁止されているAPI(OS機能)を拒否する。

【0136】次に、プロセス内メモリの参照または変更を禁止する例について説明する。

【0137】従来、アプリケーションが明示的に拒否しない限り、プロセス内メモリの参照／変更を禁止することができなかった。本発明では、プロセス内メモリの参照／変更APIを監視／制御することで、他のアプリケーションからの参照／変更を禁止することができる。

10 【0138】その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

【0139】(1) プロセス管理API

OpenProcess

CreateProcess

CloseHandle

(2) メモリ操作API

ReadProcessMemory

WriteProcessMemory

ReadProcessMemoryVlm

20 WriteProcessMemoryVlm

このようなAPIの監視によってプロセス内メモリの参照または変更を禁止する印刷を禁止する場合、具体的な方法として次の方法がある。

【0140】＜方法＞アクセスが禁止されているアプリケーションのプロセス内メモリにおいて、メモリ操作APIが要求された際に、アクセス違反エラーを返す。

【0141】次に、ブラウザに表示したWebページの印刷や保存や外部装置への出力を禁止する例について説明する。

【0142】従来、閲覧や再生のみを許可したWebページでも、実際にはブラウザソフトによって印刷や保存が可能であった。WebページをロードするためのネットワークリソースにアクセスするAPIを監視し、ブラウザが行なう印刷や保存を監視／制御することにより、印刷や保存や外部装置への出力操作を禁止することができる。その場合に、監視／制御するAPIとして次のようなものがある。

【0143】Windowsの場合

(1) 通信API

40 WSASStartup

accept

bind

connect

gethostbyname

gethostbyaddr

getprotobyname

getprotobynumber

getservbyname

getservbyport

50 getpeername

```

getsockname
gethostname
getsockopt
setsockopt
recv
recvfrom
socket
select
send
sendto
WSASend
WSASendTo
WSAAsyncSelect
WSAAsyncGetHostByAddr
WSAAsyncGetHostByName
WSAAsyncGetProtoByNumber
WSAAsyncGetProtoByName
WSAAsyncGetServByPort
WSAAsyncGetServByName
WSACancelAsyncRequest
WSASetBlockingHook
WSAUnhookBlockingHook
WSACleanup
closesocket
shutdown
(2) その他、前述のファイル、印刷、外部装置への操
作を禁止する場合のAPI
UNIXの場合
(1)
accept
bind
connect
gethostbyname
gethostbyaddr
getprotobyname
getprotobynumber
getservbyname
getservbyport
getpeername
getsockname
gethostname
getsockopt
setsockopt
recv
recvfrom
socket
select
send
sendto
closesocket

```

shutdown

(2) その他、前述のファイル、印刷、外部装置への操作を禁止する場合のAPI

このような通信APIを監視し、印刷や保存や外部装置への出力を禁止する方法として、次の方法がある。

【0144】まず、Webページ内に記述された禁止指定を読み取る。具体的には、httpプロトコルまたは同等のプロトコルのデータを監視し、その中のWebページデータ部分に印刷や保存の禁止指定タグが含まれてい
10 れば、そのWebページは印刷や保存が禁止されていると判断する。または、権限の獲得を利用者に求め、獲得できなかった場合に印刷や保存が禁止されていると判断する。しかし、獲得できた場合には、印刷や保存が禁止されていないものと判断する。すなわち、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する。

【0145】印刷や保存や外部装置への出力が禁止されているページを表示しているブラウザが、印刷や保存を行なおうとした場合、前述した印刷やファイルの保存や
20 外部装置への出力を禁止する方法を用いて、それを禁止する。

【0146】ここで説明したWebページの例は、そのしくみの類似性により、容易にデジタルテレビジョンのコンテンツにおいても利用できるものである。

【0147】次に、リソース管理プログラムを応用した例を示しておく。

【0148】図6は、リソース管理プログラム203が管理しているリソースのアクセス状況を履歴管理プログラム601に転送し、履歴管理データベース(DB)6
30 02に格納しておき、必要に応じて、図8に示すようなアクセス監視履歴として画面表示する構成を示したものである。通報プログラム603は、不正なアクセスがあった場合にシステム管理者の端末に対し、図7(B)で示すような内容の不正アクセス通知画面を送信し、表示させるものである。

【0149】なお、一般ユーザが不正アクセスを行なった場合には、図7(A)で示すような画面表示が行われる。

【0150】なお、上記の説明においては、アクセス権限管理テーブル2035を参照してアクセス権限の有無を判定するようにしているが、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権限を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するようにすることもできる。
40

【0151】また、上記の説明において用いたネットワークリソースとは、通信媒体、デバイス、アクセスポイント、デジタルテレビジョンのチャンネル、通信データまたはコンテンツなど、OSが管理しているリソース
50 のうちネットワークに関するものである。

【0152】以上のように、第1実施形態においては、リソース管理プログラム203によって、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部装置等のOSが管理しているコンピュータリソースに対するプロセスまたはOSからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する。判定の結果、アクセス権限があれば当該操作要求通りにOSに渡し、その結果を要求元プロセスに返す。一方、アクセス権限がなければ当該操作要求を拒否するようにする。これにより、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

【0153】また、リソース管理プログラム203を既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権限の範囲を拡張することが可能になる。

【0154】さらに、要求元のアプリケーションがアクセス違反に対応する機能を有していない場合であっても、ダミーのコンピュータリソースへの操作要求に変換してOSに渡すようにしたため、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができる。

【0155】なお、リソース管理プログラム203は、CD-ROM等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

【0156】また、第1実施形態で例示したAPIについては、その一例を示しただけであって、OSのバージョンアップなどによって追加された場合でも容易に対応できることは言うまでもない。

【0157】

【第2実施形態】図10は本発明による第2実施形態のシステム構成を示す図である。

【0158】図10において、11は、先に説明したセキュリティ環境における本発明のコンピュータアーキテクチャの構造を有するサーバを示している。本構成は、第1実施形態のリソース管理プログラム203によって実現されるハミングヘッズセキュリティ管理システム（H、Hシステム）の全体構成を示すもので、本発明によるコンピュータアーキテクチャのHierarchyを示している。

【0159】201はOSであり、先に説明したようにWindowsでも、MACでもOSはどれでもよい。本HHシステムは、OSに依存しないのが特徴である。

18のAPI1（Application Program Interface1）は、OS201の中に位置していて、OS201とのインターフェースの役割を果たす。これは、図2のOS201がアプリケーションに提供しているAPI群2012に対応する。また、リソース管理プログラム203に対応するSCM19からの要求に応じて、OS201に指示をおくる。

【0160】この場合の指示とは、クライアントへの情報の提供の方法に関するものであって、情報を一切拒否したり、閲覧のみ可としたり、コピー、メール、転送等の許可を行なう。

【0161】19のSCM（Security Control Management）は、図2のリソース管理プログラム203に対応し、本発明の主旨であるH、H（ハミングヘッズ）セキュリティモジュールを示す。これは、OS201、APL21（アプリケーション・ソフトウェア）の処理を監視し、何らかの条件で、APL21によるリソースへのアクセスの許可、不許可を決める。12はアクセス権限管理テーブルであり、図2のアクセス権限管理テーブル2035を拡張したものである。特に、このアクセス権限管理テーブル12では、本システムにどのような形でクライアントがアクセス可能か、を判断する。また、クライアントがアクセスした場合、アクセス権限管理テーブル12の中に人の名、電話番号、あるいはID番号を保持し、それらでアクセスしたクライアントの位置付けと重みを判断する。

【0162】尚、ここで説明するクライアントとは、サーバ11に対する1つの端末あるいは、その端末を使用する複数ユーザそれぞれあるいはそれらの一部あるいはすべてを示すものである。

【0163】特に、クライアントの要求をそのまま受け入れるか、条件をつけて許可するかは、アクセス権限管理テーブル12に格納されているクライアントの個人データによって判断する。尚、情報の提供を要求通りクライアントに提供できないが、課金することによって提供できることもある。この場合は、クライアントの個人データに課金の有無に応じてクライアントの要求をそのまま受け入れるか、条件をつけて許可するかを設定を行なっておく。

【0164】20のAPI2（Application Program Interface 2）は、APL21とSCM19間のAPIとして機能し、クライアントのアクセスを監視していて、アクセスがあればOS201にわたす。また、OS201のコントロール下にある外部装置の監視も行なう。OS201の要求する全てのリソースが対象になる。また、API2（20）は、図6の履歴管理プログラムの機能を有し、必要に応じて履歴ファイル14に、クライアントからのアクセス、要求の履歴を記憶する。

【0165】21のAPLは、各種のアプリケーション

プログラムであって、例えばマイクロソフト社のOffice 2000、Word、Excel、Power Pointなどの類である。クライアントは文章、図、あるいは静止画、動画、音声、音楽等の情報の利用・再生をOSのコントロール下で行なう。13はAPL 21で作成されたファイルであり、例えば、各種のアプリケーションソフト、クライアントの作成したファイル群である。

【0166】22は、例えば、SCM 19を搭載したサーバ11と、外部装置とを接続するインターフェース（I/F）であり、本例では、通信ネットワーク15、ドライバソフト16を介して外部装置（クライアント28、ユーザの画面23、プリンタ24、Fax/コピー機25）に接続している。

【0167】又、他のクライアントは通信ネットワーク15を介して、23、24、25、28等の外部装置を用いて情報の提供を受けることが出来る。

【0168】26は公衆網通信インターフェースであり、27は外部装置接続用のUSB、RS 232C、IEEE 1394等のシリアル、パラレルのコネクタと接続する通信ラインである。29は外部装置との接続線であって、ドライバソフト16は、外部装置23、24、25、28がサーバ11に内蔵されているのが一般的である。

【0169】図11は、図10に示した構成において、OS 201、外部装置23、24、25、28、ファイル13とSCM 19との関係を示した模式図である。ファイル13には、クライアントによって作られた創作物、サーバ11が提供するH、Hサイト（ハミングヘッズサイト）、サーバ11から提供される各種の情報が格納されている。この情報とは、文章、図、絵、音声、静止画、動画等を含む。

【0170】SCM 19はOS 201とAPL 21の中間に位置して情報の抽出、使用について、クライアントの動きを監視している。OS 201のコントロール下で外部装置23、24、25、28への情報の出力についてクライアントの権限をチェックして、制限をくわえる。制限とは、先に説明したように情報のコピー、電子メールによる転送の許諾権を与えるものである。

【0171】アクセス権管理テーブル12には、クライアントの権限情報を格納していて、要求に応じてその都度、照合して外部装置への出力に制限をくわえる。クライアントはあらかじめ個人の情報を登録しておく必要がある。企業、法人、政府機関、自治体等であれば、部長、課長、一般職というように職位によって権限を制限したり、与えたりしてもよい。

【0172】又、外部の一般人がクライアントとしてアクセス要求する場合もある。その時には、外部に出せる情報であれば無料のものと有料のものとを層別してSCM 19が管理しておけばよい。

【0173】

【第3実施形態】実施形態1、2では、リソース管理プログラム203が事前にサーバやクライアントに搭載された環境で、本発明のセキュリティ環境を提供するものであった。しかしながら、このリソース管理プログラム203が事前に搭載されていないサーバやクライアントでは、本発明のセキュリティ環境を実現することができない。そこで、第3実施形態では、リソース管理プログラム203が事前に搭載されていないサーバやクライアントに対し、本発明のセキュリティ環境を実現するための構成について説明する。

【0174】図12は第3実施形態を示すシステム構成図である。

【0175】図12に示す構成は、プロテクション化電子情報を提供する情報処理装置310と電子情報を受け取り利用するための情報処理装置311とプロテクション化電子情報を受け取り側へ送信することが可能な通信回線312からなるシステム構成を示すものである。

【0176】提供側の情報処理装置310は、ハードディスクドライブ（HDD）3103を備えたコンピュータ（PC）3100、外部にプロテクション化電子情報を出力することが可能な外部装置（例えば、フレキシブルディスクドライブ（FDD））3102で構成され、提供対象の電子情報3101を保持している。また、通信回線312と接続する外部インターフェース（I/F）3104を有している。

【0177】尚、PC 3100は、パーソナルコンピュータやワークステーション等の汎用コンピュータであり、汎用コンピュータが標準的に装備する不図示のキーボードやマウス、ディスプレイ等を有している。

【0178】一方、受け取り側の情報処理装置311は、ハードディスクドライブ（HDD）3112を備えたコンピュータ（PC）3110、外部からプロテクション化電子情報を読み込むことが可能な外部装置（例えば、フレキシブルディスクドライブ（FDD））3113、ディスプレイ3116、プリンタやFAX、コピー機等の出力部3115、キーボードやマウス等の入力部3114で構成され、外部インターフェース（I/F）3117を介して受け取ったプロテクション化電子情報3111を保持している。また、通信回線312と接続する外部インターフェース（I/F）3117を有している。

【0179】このようにして、提供側の情報処理装置310と受け取り側の情報処理装置311は、通信回線312を利用してプロテクション化電子情報を含む各種電子情報の受け渡しが可能となっている。

【0180】PC 3100には、汎用のOSまたはプラットフォームが組み込まれており、さらに第3実施形態に係るプロテクション化プログラムが組み込まれている。

【0181】PC3110には、汎用のOSと受け取った電子情報にアクセスするためのアプリケーションが組み込まれている。

【0182】提供側では、提供する電子情報3101をプロテクション化プログラムによってプロテクション化し、プロテクション化電子情報を作成する。作成したプロテクション化電子情報を外部装置3102もしくは通信網312を介して受け取り側に渡し、受け取り側の情報処理装置311では、外部装置3113もしくは通信回線312を介してプロテクション化電子情報を受け取る。そして、受け取ったプロテクション化電子情報を実行することで、目的の電子情報を利用可能となるが、その電子情報に対するプロテクション化によって利用範囲は制限される。例えば、印刷操作の禁止や利用ユーザの限定などである。尚、この制限は、第1実施形態のリソース管理プログラム203によって実現されるものである。

【0183】このように、第3実施形態では、受け取り側に制限操作を定義したプロテクション化電子情報を渡すことによって、提供側は受け取り側の利用範囲を限定した形で電子情報を提供することが可能となる。

【0184】図13(A)は、プロテクション化電子情報の構成を示す図であり、プロテクション化電子情報320は制限プログラム321、制限属性322、制限対象の元電子情報323から構成される。また、図13(B)に示すように、制限プログラム321は展開ルーチン部3210と制限ルーチン部3211から構成される。尚、この制限ルーチン部3211は、第1実施形態のリソース管理プログラム203に対応する。

【0185】さらに、図13(C)に示すように、制限属性322は対象アプリケーション情報3220、制限操作情報32211～3221N、それに対応する制限条件情報32221～3222Nから構成される。尚、制限操作情報と制限条件情報の組は必要に応じて複数保持することがあり、図ではN組の制限操作情報と制限条件情報の組を保持している状態を示している。

【0186】制限操作情報としては、アプリケーション、OSまたはプラットフォームに実装されている機能のうち、制限したい機能を指定する。例えば、印刷、編集、表示、画面のイメージ取得、外部装置への保存などである。

【0187】制限条件としては、操作を制限するための条件を指定する。例えば、利用可能な時間の指定、利用可能なコンピュータの指定、利用可能なユーザやグループの指定、課金条件などである。

【0188】無条件に特定の操作を制限する場合は、制限条件を省略する。

【0189】また、対象アプリケーションが自明であるような場合には、対象アプリケーション情報3220は省略されることもある。例えば、Windowsでは対

象ファイルの拡張子によってアプリケーションが特定されることがあり、これは対象アプリケーションが自明なケースである。

【0190】逆に、対象アプリケーションを明示することで、電子情報にアクセスするアプリケーションを限定することが可能となる。

【0191】制限ルーチン部3211は、対象の電子情報に対する操作を監視及び制御するプログラムコード（第1実施形態のリソース管理プログラム203）が実装されており、その内容および実現方法については、第1実施形態で説明した通りである。

【0192】図14は第3実施形態におけるプロテクション化電子情報の提供手順を示すフローチャートである。

【0193】ステップS30で、対象となる電子情報323を読み込み、メモリやハードディスクなどの記憶媒体に記憶する。

【0194】この時、電子情報323を暗号化した状態で記憶する場合もある。この場合は、プロテクション化した状態では元の電子情報を読み取ることは困難となり、よりセキュリティが向上する。

【0195】ステップS31で、電子情報323に対して制限する操作およびその条件が定義された制限属性322を、ステップS30で記憶した電子情報323に付加する。また、必要であれば制限属性322に電子情報323を利用するためのアプリケーション情報を含めることもある。アプリケーション情報を含めた場合は、そのアプリケーションを使用してのみ電子情報にアクセス可能となる。

【0196】ステップS32で、電子情報323へのアクセス制御を実行する制限プログラム321を、S30で記憶した電子情報323に付加する。これによって、プロテクション化電子情報320が生成される。制限プログラム321の内容は、対象の電子情報323に対して指定した制限内容が制御可能であるプログラムコードが実装されていれば十分であるので、対象の電子情報323や制限属性322によって異なるものになっても良い。

【0197】また、制限プログラム321は、プロテクション化電子情報320を受け取る側のOSやプラットフォームで実行可能である必要があるため、受け取る側の利用環境に応じた実行可能な形式のプログラムコードにする。

【0198】ステップS33で、プロテクション化電子情報320を出力する。ここで、プロテクション化電子情報320は、ステップS30で記憶した電子情報323にステップS31およびステップS32によって制限属性322および制限プログラム321が付加されたものであり、プロテクション化電子情報320を利用する環境において実行可能な形式にする。

10

20

30

40

50

【0199】図15は第3実施形態のプロテクション化電子情報の利用手順を示すフローチャートである。

【0200】プロテクション化電子情報320は、利用環境において実行可能な形式になっているが、プロテクション化電子情報320を実行した際の処理は、制限プログラム321中の展開ルーチン部3210にあるプログラムコードによって行われる。このフロー図は、展開ルーチン部の流れを説明するものである。

【0201】なお、制限プログラム321には、展開ルーチン部3210の他に制限ルーチン部3211が含まれているが、制限ルーチン部3211はアプリケーションからのアクセスを制御するプログラムコード（第1実施形態のリソース管理プログラム203）からなっており、その詳細については、第1実施形態で説明した通りである。

【0202】ステップS401で、プロテクション化電子情報320を起動する。起動方法は利用環境によって異なるが、例えばOSが実行ファイルとして起動する場合や、WebブラウザがプラグインやJ A V A（サン・マイクロシステムズ社の登録商標）アプレットとして起動する場合がある。

【0203】ステップS402で、制限プログラム321中に含まれる制限ルーチン部3211をコンピュータ内のRAMにロードし起動する。

【0204】ステップS403は、プロテクション化電子情報320に含まれている制限属性322を取得する。制限属性322に起動するアプリケーション情報3220が含まれている場合は、そのアプリケーション情報3220を取得し起動すべきアプリケーションを特定する。制限属性322に起動するアプリケーション情報が含まれていない場合は、起動すべきアプリケーションを自動判断によって特定する。

【0205】自動判断の方法は、例えば電子情報323のタイプや拡張子からOSにて定義されているアプリケーションを取得する方法や、利用環境に応じてアプリケーションを特定する方法がある。

【0206】また、制限属性322に含まれている制限操作および制限条件を取得し、ステップS402によって起動した制限ルーチン部3211に渡す。

【0207】ステップS404で、ステップS403によって特定したアプリケーションを起動する。

【0208】ステップS405で、ステップS403によるアプリケーションの起動が成功したか失敗したかを判断する。アプリケーションの起動が成功した場合は（ステップS403でY e s）、ステップS407に進む。そして、ステップS407以降では、ステップS402によって起動した制限ルーチン部3211が、その仕組みにより、アプリケーションのアクセスに対する監視を開始し、これ以降のアプリケーションの操作に対して制御が可能となる。

【0209】ステップS403によるアプリケーションの起動が失敗した場合は（ステップS404でN o）、プロテクション化電子情報320の実行を終了する。

【0210】尚、プロテクション化電子情報320の実行を終了する際に、ステップS413において、ステップS402にて起動した制限ルーチン部3211を終了させる場合もある。

【0211】この制限ルーチン部3211を終了させない時は、以降のプロテクション化電子情報320の起動時に、同一の制限ルーチン部3211を起動させる場合、その起動が速くなるという利点がある。ステップS403によるアプリケーションの起動が失敗した場合にステップS413を実行するか否かは、利用環境に応じて選択すれば良い。

【0212】一方、アプリケーションの起動が成功した場合、ステップS407で、プロテクション化電子情報320に含まれる元の電子情報323を抜き出し、アプリケーションがアクセス可能な状態に復元する。例えば、アプリケーションがファイルの形式でアクセスするのであれば、ファイル形式に出力する。元の電子情報と同じ形式の情報に復元することで、アプリケーションからのアクセスが可能となる。

【0213】なお、図14のステップS30において電子情報323を暗号化している場合は、ステップS407にて、その電子情報323の復号も行なう。

【0214】ステップS408で、ステップS407で復元した電子情報をステップS404で起動したアプリケーションに渡す。

【0215】ステップS409で、アプリケーションが電子情報323に対して通常のアクセスを行なっている状態となる。ただし、制限ルーチン部3211によってアクセスは制御されているため、制限属性322で定義された制限の範囲でのみ電子情報323が利用できる。すなわち、プロテクション化によって禁止された操作を試みた場合、制限ルーチン部3211によって拒否される。また、課金によって操作が許可される場合もある。

【0216】ステップS410で、アプリケーションが電子情報320を解放する。一般的にアプリケーションは、電子情報320の使用が終了すると、その使用しなくなった電子情報を解放する。ファイル形式の電子情報の場合は、解放のことをクローズとも呼ぶ。

【0217】ステップS411で、ステップS410でアプリケーションが電子情報320を解放したことをトリガーにして、ステップS407にて復元した電子情報320を抹消する。

【0218】ステップS412で、アプリケーションを終了する。

【0219】ステップS413で、ステップS412のアプリケーション終了をトリガーにして、ステップS402で起動した制限ルーチン部3211を終了およびコ

ンピュータ上から解放する。

【0220】ステップS411およびステップS413は、プロテクション化電子情報320を起動し、元の電子情報をアプリケーションが利用している間に解放および抹消する処理であるが、これらの処理は省略することもできる。省略した場合も、目的の電子情報に対する操作の制限は可能であるが、これらの処理を行なうことで、元の電子情報の痕跡を残さないという利点がある。また、コンピュータ上のリソースを節約できるという利点もある。

【0221】次に、第3実施形態の具体例について説明する。

【0222】図16はファイル形式の電子情報を提供する場合の具体例を示す図である。ここでは、電子情報として、ワープロソフトで利用する文書ファイルを例に挙げている。

【0223】文書ファイルを提供する側(350)では、制限付きで提供したい文書ファイル(3501)に対して、プロテクション化を行ない(3502)、プロテクション化文書ファイル(3503)を作成し、このプロテクション化文書ファイル(3503)を利用者側に提供することで、文書ファイルに対する利用者側での操作を制限する。

【0224】提供手段としては、電子メールソフトやFTPソフトといったファイルを転送するためのソフトを利用して提供する方法(351)、フレキシブルディスクやCD-R/RWといった、記録可能かつ取り外し可能な媒体にコピーし提供する方法(352)、LANや公衆回線などのネットワークを用いたリモートファイルシステムを利用して提供する方法(353)などがある。

【0225】いずれの方法も、プロテクション化文書ファイル3503はファイル形式のまま利用者側に提供される。提供されたプロテクション化文書ファイル3503は利用者側のコンピュータで実行可能な形式をしており、実行することで、電子情報にアクセスするためのワープロソフトが実行され、すでに述べた方法によって、ワープロソフトで対象の電子情報が利用可能となる。しかも、利用中は制限ルーチン部によってワープロソフトのアクセスが制御されており、禁止された操作は拒否される。

【0226】例えば、閲覧のみ許可するために、印刷、編集または文書の転写を禁止する場合、ワープロソフトが禁止したい機能を備えたものであれば、制限ルーチン部にこれらの制御プログラムコードを含め、制限操作として印刷、編集、転写機能を指定することで実現可能となる。

【0227】また、利用時間や利用者、利用場所を限定する場合には、制限条件として、それらの条件を指定することで制限可能となる。

【0228】さらに、課金情報を制限条件に指定することで、利用者が文書ファイルを閲覧する際に、課金することも可能となる。

【0229】この例は、著作権の対象となる文書ファイルや、特定の人だけにのみ提供する場合に有効となる例である。

【0230】図17はファイル形式以外の電子情報を提供する場合の具体例を示す図である。ここでは、電子情報として、画像、音楽、動画等のマルチメディア情報を例に挙げている。

【0231】マルチメディア情報を提供する側(360)では、制限付きで提供したいマルチメディア情報(3601)に対して、プロテクション化を行ない(3602)、プロテクション化マルチメディア情報(3603)を作成し、このプロテクション化マルチメディア情報(3603)を利用者側に提供することで、マルチメディア情報に対する利用者側での操作を制限する。

【0232】提供手段としては、Webシステムを利用して提供する方法(361)、携帯電話などの携帯端末機を用いたサービスを利用して提供する方法(362)などがある。

【0233】いずれの方法も、プロテクション化マルチメディア情報3603は通信網を介して通信データとして利用者側に提供される。提供されたプロテクション化マルチメディア情報3603は利用者側のコンピュータで稼動しているWebブラウザソフトや、携帯端末機のOS上で実行可能な形式をしており、プロテクション化マルチメディア情報3603を実行することで、マルチメディア情報にアクセスするためのマルチメディアソフトが実行され、すでに述べた方法によって、対象の電子情報が利用可能となる。しかも、利用中は制限ルーチン部によってマルチメディアソフトのアクセスが制御されており、禁止された操作は拒否される。

【0234】ここで、Webブラウザや携帯端末機上で実行可能な形式としては、JAVAアプレットの形式や特定のプラグインにて実行される形式などがある。すなわち、プロテクション化電子情報3603の形式は、利用者側のプラットフォームで実行可能な形式であり、対象のアプリケーションが起動できるものであれば良い。

【0235】なお、実行可能な形式がファイル形式であれば、プロテクション化文書ファイル3503で説明した方法と同じ方法にて実現される。

【0236】例えば、閲覧のみ許可するために、印刷、編集またはマルチメディアの転写を禁止する場合、マルチメディアソフトが禁止したい機能を備えたものであれば、制限ルーチン部にこれらの制御プログラムコードを含め、制限操作として印刷、編集、転写機能を指定することで実現可能となる。

【0237】また、利用時間や利用者、利用場所を限定

する場合には、制限条件として、それらの条件を指定することで制限可能となる。

【0238】さらに、課金情報を制限条件に指定することで、利用者がマルチメディア情報を利用する際に、課金することも可能となる。

【0239】この例は、ライブ情報などをリアルタイムで提供する場合のようにファイル形式で提供が困難なマルチメディア情報や、Webシステムを利用した不特定多数に対する提供において課金するような場合に有効となる例である。

【0240】以上説明したように、第3実施形態によれば、プロテクション化電子情報を作成することで、事前にセキュリティが確保されていない環境においても、必要に応じて、所望のセキュリティを確保した環境を提供することができる。

【0241】以上の第3実施形態で例示したプロテクション化電子情報については、その一例を示しただけであって、電子情報の利用環境に合わせた実行可能な形式であれば良く、OSやプラットフォームがバージョンアップなどによって変更された場合でも容易に対応でき、さらに制限プログラムの機能の範囲において、制限する操作を拡張できることは言うまでもない。

【0242】また、対象となる電子情報も、例に示したもの以外に適用可能な電子情報は多くあり、プロテクション化可能な電子情報であれば同様に制限をかけることが可能であることは言うまでもない。

【0243】なお、本発明におけるプロテクション化プログラムは、CD-ROM等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

【0244】

【第4実施形態】第4実施形態は、第1～第3実施形態の適用例について説明する。特に、第4実施形態では、イントラネット等の広域な通信環境に第1～第3実施形態を適用した例である。図18は第4実施形態を示すシステム構成図である。通信ネットワーク15は公衆網であり、インターネットIP、電話網PSTN、XDSL網、デジタル網ISDN、B-ISDN、ATM、モバイル網、衛星網等を使用している。31は公式のWebサイトであり、例えば、NTTドコモ社のiモードサイトがある。32はモバイル無線網のアンテナであり、第4実施形態では、iモードサイトに接続している。もちろんPHS、他のPDC(Personal Digital Cellular)も使用できる。特に、IMT2000は高速なので動画の伝送に優れている。

【0245】33は第2実施形態で説明したサーバ(以下、H. Hサーバ)を有するH. Hサイトであり、各種情報提供を行う。このH. Hサイト33は、先に説明し

たようにセキュリティを万全にしたシステムであり、クライアントの権限によって制限を設けるものである。

H. Hサイトは、第2実施形態で説明したSCM19をインプリメントしたソフトを搭載したサーバを使用している。

【0246】34はデータベースのサイトであり、各種のビジネス、研究等に必要情報が格納してあって、H. Hサイト33を介して使用できる。35はWebキャストであり、デジタル放送をH. Hサイトを通して利用できる。36は銀行、クレジット会社等の金融機関のサイトであり、H. Hサイト33を使用して課金された場合、使用料の徴収をおこなう。

【0247】37はWeb上に設けられたモールであり、H. Hサイト33を通してショッピングができる。購入の支払いは金融機関のサイト36よりおこなう。

【0248】Web上で商品を買ったり、デジタル放送を見たり聞いたりして、課金が発生したときにはH. Hサイト33を介しているの、利用者であるクライアント、それにサービスの提供者はセキュリティが万全であるから安心して使用できる。

【0249】38はH. Hサイト33の利用者のための端末機器をコンビニ、街角、広場に設置した例である。図示してないがプリンタ、コピー機等も接続している。39は学校、研究機関を、40は工場、オフィスを示し、それぞれH. Hサイト33の利用者のための端末機器が設定されている。

【0250】41は一般家庭でのH. Hサイト33の利用者のための端末機器の設置例であり、45は、ホームサーバを示す。近年、在宅で仕事をする人がふえてきた。通信回線の発展の恩恵によるものであって、企業内のデータ、情報を活用する場合、本発明によるセキュリティの効果が発揮する。46はホームルータである。

【0251】42は携帯情報端末機器であり、モバイル機器ともいう。携帯情報端末機器42の普及は顕著で、特にiモードの発展は急速にたちあがった。HTMLのブラウザに電子メールを送信することが可能で、これをもってH. Hサイト33にもアクセスできるから利便性はよい。さらに、PalmOSに見られるようにPDA(携帯情報端末機器)の使い勝手もよい。プリンタ、インターネットカメラ、デジタルカメラを搭載したり接続することもできる。

【0252】43はクライアント(ユーザ)である。図18では、モバイルとしてクライアント43は場所を問わず、何処でも仕事ができる。当然H. Hサイト33を利用することで、そのセキュリティである権限制限機能が発揮されるから、図示してない企業のイントラネットも容易に使用できる。

【0253】44は車載移動体であり、モバイルインターネットによって同様にH. Hサイト33からのサービスを受けることができる。

【0254】尚、第4実施形態では、H、Hサイト33にH、Hサーバを構成した例を説明したが、Webサイト31上にこのサーバを構成しても良い。また、第3実施形態によるプロテクション化電子情報を作成するためのプロテクション化プログラムを適用する場合は、例えば、H、Hサイト33やWebサイト31上に構成し、必要に応じて、利用者が利用することになる。

【0255】

【第5実施形態】第5実施形態は、第1～第3実施形態の別の適用例について説明する。特に、第5実施形態では、企業内のイントラネットに第1～第3実施形態を適用した例である。

【0256】図19は第5実施形態を示すシステム構成図である。

【0257】尚、図19において、第4実施形態と同じ構成要素については、同じ参照番号を付加し、その詳細については省略する。

【0258】通信ネットワーク15より回線26を介してルータ51に接続されている。52はWWWサーバであり、53はファイアウォールである。ファイアウォール(F/W)53のには、H、Hサーバ55に接続されている。67はWWWサーバとF/W53を接続する接続線であり、66はF/W53とH、Hサーバ55を接続する接続線である。

【0259】56はH、Hサーバ55とLAN54で接続されている企業のデータベースである。このデータベース56には、顧客のリスト、営業情報、工場であれば生産、製造の技術情報、設計開発の情報等企業活動に必要な各種のデータ、および情報が格納されていてクライアントである企業の社員は先に説明したような、権限に応じて制限付きで利用できる。これらの情報は、職能階層に応じて利用できる情報とできない情報がある。場合によっては代表権のある役員しか開示できない情報もあって、H、Hサーバ55によって適切な制限下の元で管理することが可能である。

【0260】企業内LAN54を介して接続される57、58、58mnは、企業内のクライアントPC、サーバである。59は多機能電話機、60はプリンタ、FAX/コピー機である。61は携帯情報端末機器(例えば、PDA)、62は携帯電話機、63はモバイルノートPCを示す。これらの機器は社内、構内モバイル機器として用いる。65は構内移動車載端末を示す。64は企業内、構内モバイル端末機器用のアンテナを示す。

【0261】本イントラネットは、企業だけでなく法人、研究機関、教育機関でも使用できるのをはじめ、企業外からもアクセスできる。外からの使用の場合はセキュリティを確保しつつ内部の情報を提供するということが可能になる。ゆえに、本発明によるシステムはきわめて有効である。

【0262】尚、第5実施形態では、イントラネット内

にH、Hサーバ55を構成した例を説明したが、H、Hサーバ55が実現するセキュリティ機能を企業LAN54上のクライアントに構成しても良い。また、第3実施形態によるプロテクション化電子情報を作成するためのプロテクション化プログラムを適用する場合は、例えば、H、Hサーバ55上に構成し、必要に応じて、利用者が利用することになる。

【0263】

【第6実施形態】第6実施形態は、第1～第3実施形態のさらに別の適用例について説明する。特に、第6実施形態では、SOHO等のエンドユーザ環境に第1～第3実施形態を適用した例である。

【0264】図20は第6実施形態を示すシステム構成図である。

【0265】尚、図20において、第4実施形態と同じ構成要素については、同じ参照番号を付加し、その詳細については省略する。

【0266】先に説明したようにITの普及によって、家庭で就労する人が増えてきた。我が国でもすでに60万人を超えたとされている。少子高齢化と共にこの傾向は増加の一途にあるといえる。

【0267】図20において、エンドユーザがいる家41は、ホームルータ72を介して公衆回線26に接続される。ホームルータ72はホームLAN73に接続されている。ホームLAN73は有線LANだけではなく、ブルートース、IrDAを使用した無線LANでもよい。74はPCまたはホームサーバ、75は大画面付きの多機能電話機、76はTV、77は音響AV機器、78は携帯情報端末機器を示す。71はアンテナで公衆無線網との接続を行なう。41は家、家庭を示す。

【0268】在宅就労は各種の企業情報、機密情報を扱うのでセキュリティの確保は最重要課題である。第6実施形態では、公式Webサイト31からH、Hサイト33を通して情報の授受を行なうから安全である。又、仕事だけでなく娯楽としてのコンテンツをネットワークから配信を受ける環境になってきた。Webキャスト35からTVや音楽の配信を受けて、TV端末76、AV機器77、携帯情報端末機器78で閲覧、鑑賞を行なうことができ、生活を豊かにすることができる。

【0269】有料娯楽コンテンツの提供をネットワーク上のサイトから受けた場合、料金の支払いが生ずる。この場合、H、Hサイト33を利用することで、例えば、クレジットカード番号を入力して金融機関のサイト36から利用料の自動引き落としが可能になる。この場合、なりすましを防止するために個人認証が必要になる。個人認証の方法は各種提案されているが、ID番号、電話番号のほかに機密性の高い場合は公開鍵を使用するものもよい。なお、ホームサーバ74をH、Hサーバを搭載して安全を確保してもよい。組織に属して家庭で就労する場合、ホームサーバ74は企業から提供されたものを使

用して家庭就労するという、条件を設けるのも一つのホームワーキングの方法である。

【0270】また、第3実施形態によるプロテクション化電子情報を作成するためのプロテクション化プログラムを適用する場合は、例えば、H. Hサイト33やWebサイト31上に構成し、必要に応じて、利用者が利用することになる。

【0271】次に、第6実施形態におけるセキュリティ確保についての流れ、ユーザ、クライアントに制限と課金を課す流れについて説明する。

【0272】図21は第6実施形態を実現するためのフローチャートである。

【0273】尚、図21では、便宜上、H. Hサイト33と、そのH. Hサーバの管理下にあるH. Hサイト33にアクセスするクライアント間の処理として説明するが、通信ネットワーク15上のH. Hサーバとクライアント間の処理で図21の処理が実現されても良い。ステップS81で、クライアントが情報を得るためにH. Hサイト33にアクセスする。ステップS82で、H. Hサイト33で、アクセスしてきたクライアントの個人情報10を検索、照合する。

【0274】ステップS83で、クライアントからの情報の特定を行なう。ここでいう特定とは、機密度の程度と、アクセスしてきたクライアントの職位の階層によって権限の制限を受けるのが特徴である。クライアント、ユーザは組織に所属しているものであれば、職位の階層は自動判別できる。一般からのアクセスも可能であるから提供できる情報と出来ないものを区別する。また、無料で提供できる企業のカatalog類とか宣伝類のほか有料で頒布できる情報もある。有料でも価値の高いものは、課金の程度を変えて頒布するのを特徴とすれば、本H. Hサイト33はビジネスとして成立する。

【0275】ステップS84で、H. Hサイト33にアクセスしてきたクライアントからの要求にこたえられるか否かを判定する。

【0276】ステップ84で、判定の結果、そのクライアントに情報を提供しても良い場合、ステップS85で、OKの返事、表示を出す。次に、ステップS86で、例えば、クライアントが要求情報のコピーと電子メールでの他人への転送を要求する。ステップS87で、クライアントの職責、権限をH. Hサイト33によって判定する。先に説明したが、本発明では個人の権限によって情報の利用を制限するものである。

【0277】判定の結果、クライアントの要求を了承する場合、ステップS88で、コピーもメール転送もOKである旨をクライアントの画面に表示する。尚、この要求が了承される場合とは、例えば、クライアントが高位な権限をもっているか、要求情報の機密性の低いものであったと判断される。

【0278】ステップS89で、クライアントがどんな

情報、ドキュメントをいつ、コピーしたか、メール転送したかの履歴がH. Hサーバ33に記録される。

【0279】ステップS90で、H. Hサーバ33での履歴の管理が終了し、要求情報の提供する条件が満たされるので、クライアントへ要求情報を提供する。

【0280】一方、ステップS84の判定の結果、そのクライアントに情報を提供できない場合、ステップS91で、クライアントへ要求が拒否される旨を通知する。ステップS92で、クライアントは、ID番号として、電話番号、保険証の番号、免許証、年金番号等を入力する。このようなID番号を入力する必要があるクライアントとは、H. Hサイト33に初めてアクセスしてきたクライアントや、H. Hサイト33を利用しない一般のクライアントが想定される。

【0281】そして、ステップS93で、H. Hサイト33は、入力されたID番号に基づいて、以降の処理の実行の可否を判定する。実行を拒否する場合、処理を終了する。一方、実行を許可する場合、ステップS85に進む。

【0282】お金を払えば提供を許可する情報であれば、課金の金額をクライアントに知らせる。金額は情報、ドキュメントの機密度、重要度によって価値は変わり、金額も異なる。

【0283】つまり、ステップS93は、課金を情報公開の条件としない情報であったり、有料の場合はクライアントが必要としない情報であったり、課金金額によってはクライアントが必要とする情報であったりする場合を想定して構成されている。このようにして、入手の許可が可能であれば、ステップS85へ進み、許可できないければ、処理を終了する。

【0284】一方、ステップ87の判定の結果、クライアントの要求が了承できない場合、ステップS94に進む。ステップS94では、欲しい情報、ドキュメントのコピー、電子メール転送がS87の判定によって不可と判定されているが、クライアントの画面で閲覧することを許可し、そのような表示をクライアントの画面に出力する。このため、閲覧用情報がクライアントに送られるが、H. Hサイト33によってその情報がコントロールされているため、クライアントの画面に情報が表示されていても、その情報のコピーと電子メール{で}の転送はできない。

【0285】ステップS95で、H. Hサイト33に先に説明したような履歴を管理する。ステップS96で、クライアントの画面に要求のあった情報が表示される。ここで、クライアントによっては、どうしてもコピー、電子メールでの転送をしたい情報もある。そこで、クライアントは、ここであらためてサイト、サーバに許可の要求をだすことが可能である。つまり、ステップS97で、課金による情報の提供を申請する。このステップではクライアントの職責、階層は、H. Hサイト33に

認知されているから金額の程度によって、許可できる場合もある。

【0286】課金すれば提供できるとH、Hサイト33が判断した場合、金額を提示する。課金しても提供できないとH、Hサイト33が判断すれば、ステップS98で、この処理はクライアントへの操作拒否の通知画面表示のみで終了する。また、情報、ドキュメントの程度に応じて表示時間に制限を加えてもよい。所定時間内の表示を行って、より長時間見たい場合は課金制度を導入するのち方法である。

【0287】この場合、ステップS99、ステップS100で、H、Hサイト33からより長時間の表示と課金の有無をクライアント、ユーザに問い合わせる。H、Hサーバ33とクライアントが了解すれば、ステップS101で画面表示を長時間行なう。

【0288】H、Hサーバ33の課金とクライアントの了解が得られない場合は、所定時間のみの表示でこの処理は終了する。

【0289】以上説明したように、第1実施形態ではアクセス権限をOSやそのプロセスを変更しないでクライアントに対して制限して不正行為を防止する例を説明した。また、第2実施形態では、H、Hサーバのシステム構成を説明した。また、第3実施形態では、第1実施形態で実現されるセキュリティ環境を、任意の利用者に提供する構成を説明した。

【0290】第4実施形態では、通信ネットワーク、特にインターネットを中心にして社会環境で発揮するH、Hサイトのシステム構成を説明した。

【0291】第5実施形態では、企業内、工場、学校、研究機関、団体等のイントラネットに本H、Hサーバの応用について説明した。さらに、第6実施形態では、ホームオフィス、在宅就労における本H、Hサイトの応用について説明した。

【0292】なお、図21のフローチャートは、H、Hサーバ、サイトを介して情報、ドキュメントの閲覧、コピー、電子メール転送について説明してあるが、図18で説明したWebキャストからのデジタル放送の配信、各種無料有料コンテンツからの配信による課金システムにも適用することが可能である。

【0293】尚、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に配給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【0294】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0295】プログラムコードを供給するための媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R/RW、DVD-ROM/RAM、磁気テープ、不揮発性のメモ리카ード、ROMなどを用いることができる。

【0296】また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOSやプラットフォームなどが実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0297】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0298】本発明を上記媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【0299】

【発明の効果】以上の説明から明らかなように、本発明は、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部装置等のOSが管理しているコンピュータリソースに対するプロセスまたはOSからの操作要求をコンピュータリソースにアクセスする前に捕捉する。次に、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する。判定の結果、アクセス権限があれば当該操作要求通りにOSに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにする。そのため、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

【0300】また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権限の範囲を拡張することが可能になる。

【0301】また、リソース制御プログラムを既存の環境に組み込むだけで、各種の不正アクセスを制限することができ、従来のアクセス権限の範囲を拡張することが可能になる。

【0302】さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することが

できるなどの効果が得られる。

【0303】さらに、急速に進展しているeビジネスに本発明による権限制限システムを応用すれば、不正アクセスの防止、各種有料コンテンツの配信による課金に効力を発揮する。急激な高齢化社会の到来に伴い、在宅就労も重要な課題になってきた。

【0304】本H. Hシステムの導入によって、安全に企業のドキュメント、データ、情報が家庭内で取り出せて、家庭内作業と成果をWebサイト、企業に送ることも可能になる。

【0305】また、電子情報に制限プログラム及び制限属性を付加することでプロテクション化し、プロテクション化電子情報を利用することで電子情報への操作を制限することができる。

【0306】また、制限プログラムは、電子情報を受け取る側のコンピュータ上で実行可能な形式にすることにより、受け取り側の既存の環境にあらかじめ制限プログラム等を組み込む必要がなく、上述したような各種の不正アクセスを制限することができ、既存のアクセス権限の範囲を拡張することが可能になる。

【0307】さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。

【0308】例えば、著作権が適用される場合など利用範囲を制限したい電子情報を提供するにあたって、プロテクション化した電子情報を提供することにより、受け取った側での利用範囲を制限できるといった効果が得られる。

【図面の簡単な説明】

【図1】(A)本発明の実施環境の第1実施形態を示すハードウェア構成図である。

(B)本発明の実施環境の第1実施形態を示すハードウェア構成図である。

【図2】本発明の第1実施形態におけるリソース管理プログラムの機能構成及びOSとアプリケーションとの関係を示す図である。

【図3】本発明の第1実施形態におけるアクセス権限管理テーブルのデータ構成例を示す図である。

【図4】本発明の第1実施形態におけるAPIの監視／制御の第1の基本型を示すシーケンス図である。

【図5】本発明の第1実施形態におけるAPIの監視／制御の第2の基本型を示すシーケンス図である。

【図6】本発明の第1実施形態におけるアクセス履歴を記録する機能を示すブロック構成図である。

【図7】(A)本発明の第1実施形態における不正アクセスを示す画面例を示す図である。

(B)本発明の第1実施形態における不正アクセスを通知する画面例を示す図である。

【図8】本発明の第1実施形態におけるアクセス監視履歴の表示画面の例を示す図である。

【図9】アクセス制限対象となるリソースへの実際のアクセス方法の例を示す図である。

【図10】本発明の第2実施形態のH. Hサーバの構成を示す図である。

【図11】本発明の第2実施形態のSCMとOS、ファイル、外部装置との関係を示す図である。

【図12】本発明の第3実施形態を示すハードウェア構成図である。

【図13】(A)本発明の第3実施形態におけるプロテクション化電子情報の構成を示す図である。

(B)本発明の第3実施形態における制限プログラムの構成を示す図である。

(C)本発明の第3実施形態における制限属性をの構成を示す図である。

【図14】本発明の第3実施形態におけるプロテクション化電子情報の提供手順を示すフローチャートである。

【図15】本発明の第3実施形態におけるプロテクション化電子情報の利用手順を示すフローチャートである。

【図16】本発明の第3実施形態におけるファイル形式の電子情報を提供する場合の具体例を示す図である。

【図17】本発明の第3実施形態におけるマルチメディア情報を提供する場合の具体例を示す図である。

【図18】本発明の第4実施形態を示すシステム構成図である。

【図19】本発明の第5実施形態を示すシステム構成図である。

【図20】本発明の第6実施形態を示すシステム構成図である。

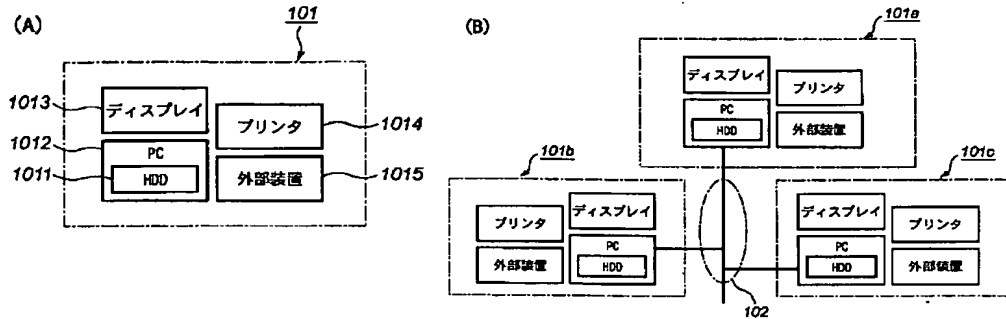
【図21】ユーザ、クライアントへの制限と課金のプロセスを示すフローチャートである。

【符号の説明】

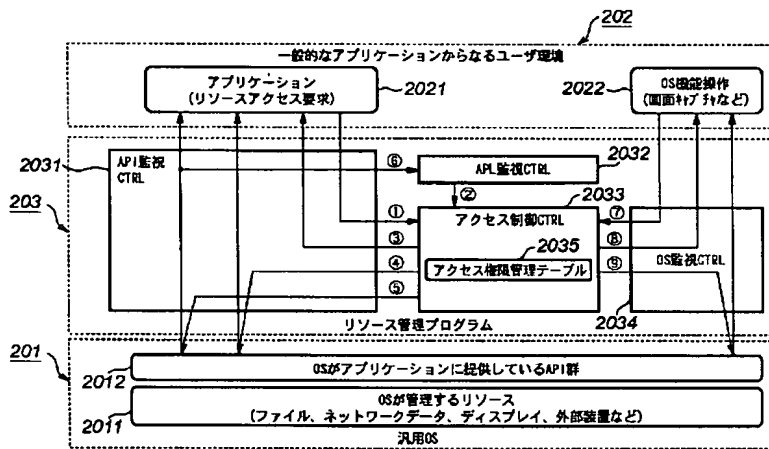
- 101 コンピュータ
- 102 ネットワーク
- 201 汎用OS
- 203 リソース管理プログラム
- 601 履歴管理プログラム
- 602 履歴DB
- 603 通報プログラム
- 2031 API監視コントローラ
- 2032 API監視コントローラ
- 2033 アクセス制御コントローラ
- 2034 OS監視コントローラ
- 2035 アクセス権限管理テーブル
- 11 H. Hサーバ
- 12 アクセス権限管理テーブル
- 13 ファイル
- 14 履歴ファイル
- 15 通信ネットワーク
- 16 外部装置ドライバソフト
- 17 汎用OS

18	API1 (Application Program Interface 1)	63	ノートPC
19	SCM (Security Control Management)	64	構内無線アンテナ
20	API2 (Application Program Interface 2)	65	構内移動車載端末機器
21	APL (Application Program Logic)	66、67	接続線
22	外部装置インターフェース	71	ホーム無線アンテナ
23	画面端末装置、TV、PDA、大画面付多機能電話機	76	TV
24	プリンタ	77	音響機器
25	Fax/コピー機	310	電子情報を提供する側の情報処理装置
26	公衆網通信インターフェース	311	電子情報を受け取る側の情報処理装置
27	通信ライン	312	通信ネットワーク
28	クライアント	3100、3110	コンピュータ
31	公式Webサイト	3101	電子情報
32	無線基地局	3102、3113	取り外し可能ディスクドライブ
33	H、Hサイト	3103、3112	ハードディスクドライブ
34	データベースサイト	3104、3117	外部インターフェース
35	Webキャスト	3111	プロテクション化電子情報
36	金融機関	3114	入力部
37	Webモール	3115	出力部
38	コンビニ、街角ターミナル	3116	ディスプレイ
39	学校、研究機関	20 320	プロテクション化電子情報
40	企業、工場、オフィス	321	制限プログラム
41	家庭、在宅就業	322	制限属性情報
42、78	携帯情報端末機器、携帯電話機、PDA	323	元電子情報
43	ユーザ、クライアント	3210	展開ルーチン部
44	車載移動端末機器	3211	制限ルーチン部
45、74	ホームサーバ	3220	対象アプリケーション情報
46、72	ホームルータ	32211	制限操作情報1
51	ルータ	3221N	制限操作情報N
52	Webサーバ	32221	制限条件情報1
53	ファイアウォール	30 3222N	制限条件情報N
54	LAN (Local Area Network)	350、360	電子情報提供側
55	H、Hサーバ	3501	一般的な文書ファイル
56	データベース	3502、3602	プロテクション化の処理
57、58、58mn	PC、サーバ	3503	プロテクション化文書ファイル
59、75	多機能電話機	351	メールやFTP等による情報提供方法
60	Fax、プリンタ、コピー機	352	FD等の記憶媒体を利用した情報提供方法
61	携帯情報端末機器	353	ネットワークにて共有
62	携帯電話機	354、363	電子情報利用者側
		3601	画像、音楽、動画等のマルチメディア情報ファイル
		40 3603	プロテクション化マルチメディア情報
		361	Webページにて公開
		362	携帯用端末へのサービス

【図1】



【図2】

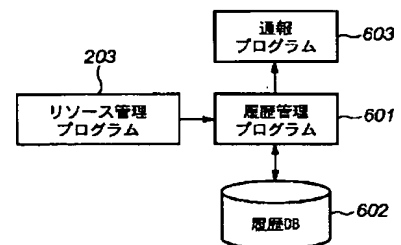


【図3】

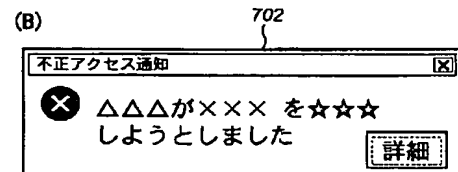
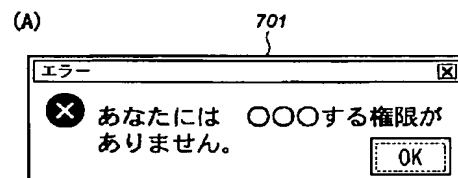
アクセス権管理テーブル

20351	20352	20353	...	2035n
リソース指定情報A	条件A	アクセス権限情報A1	...	アクセス権限情報An
リソース指定情報B	条件B	アクセス権限情報B1	...	アクセス権限情報Bn
リソース指定情報C	条件C	アクセス権限情報C1	...	アクセス権限情報Cn
...

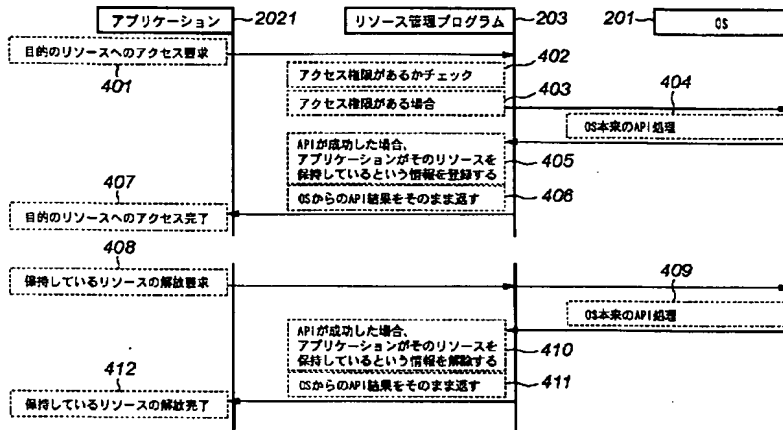
【図6】



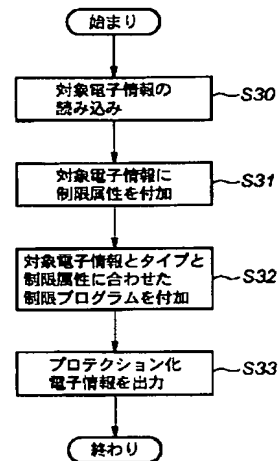
【図7】



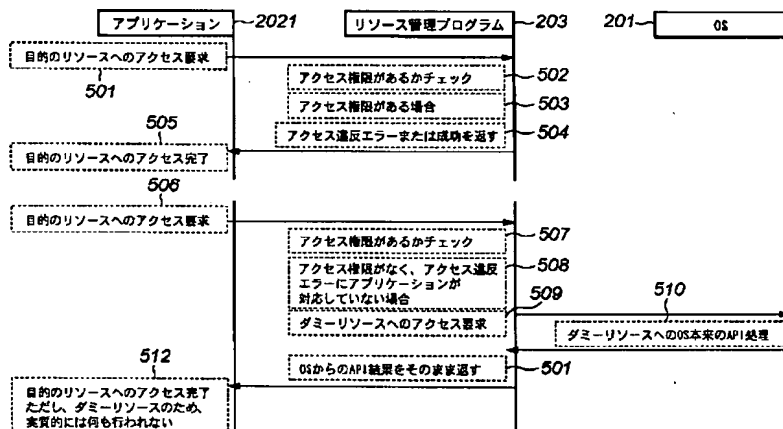
【図4】



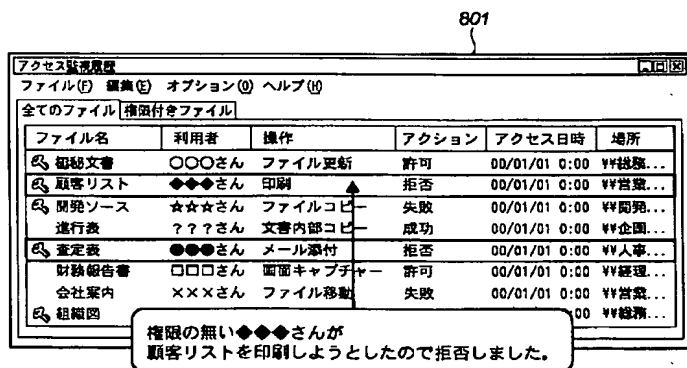
【図14】



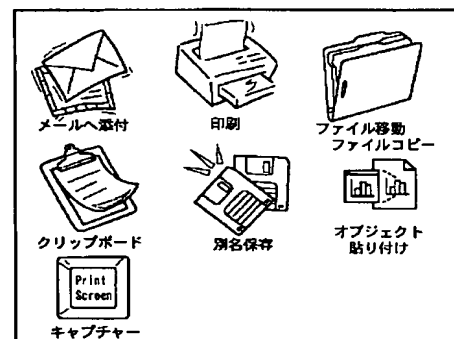
【図5】



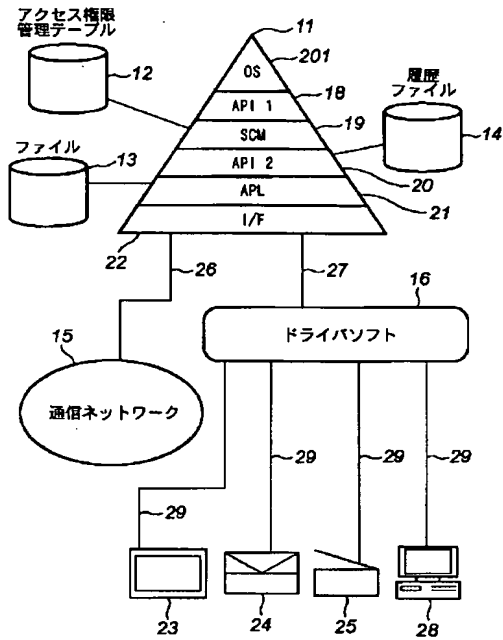
【図8】



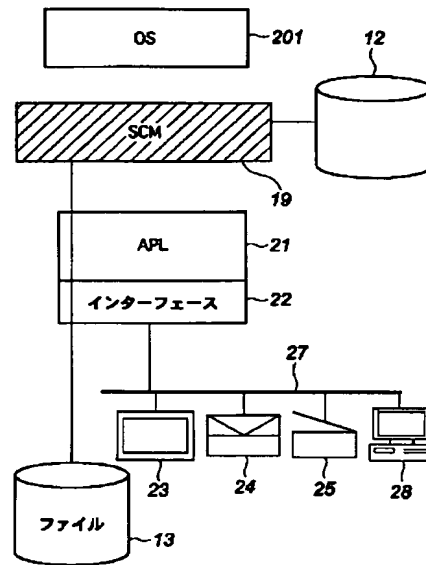
【図9】



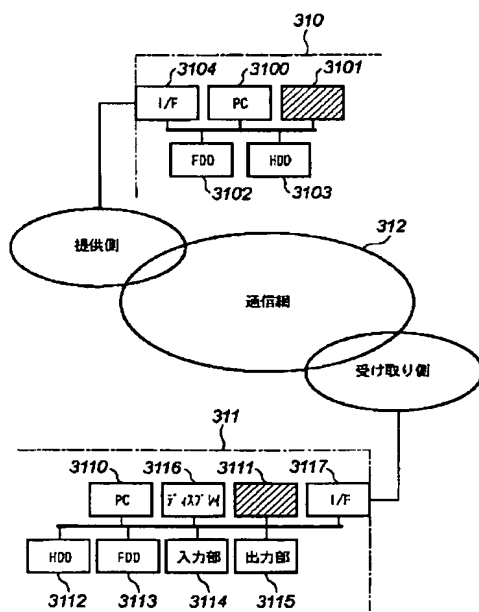
【図10】



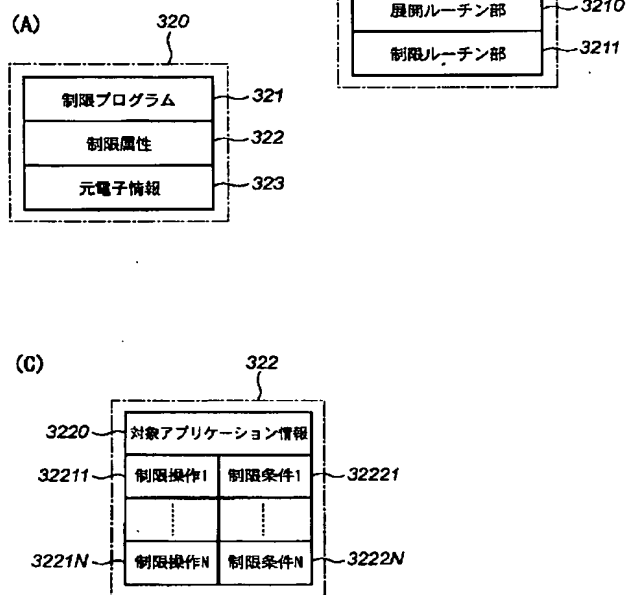
【図11】



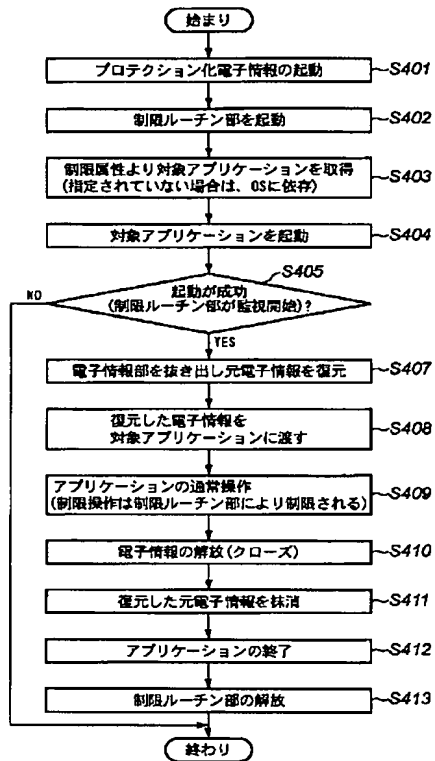
【図12】



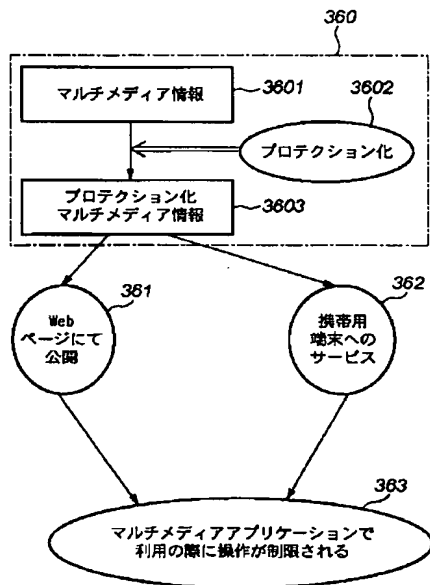
【図13】



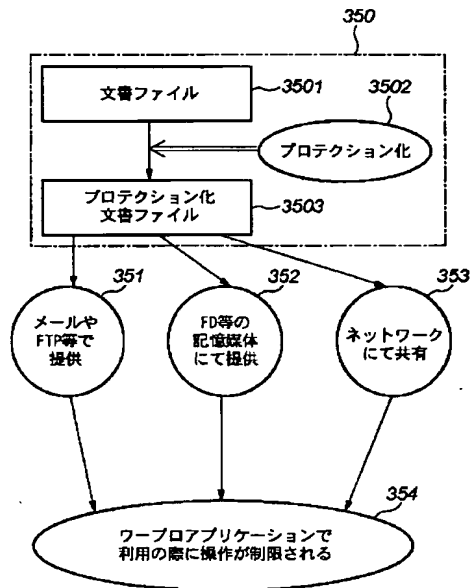
【図15】



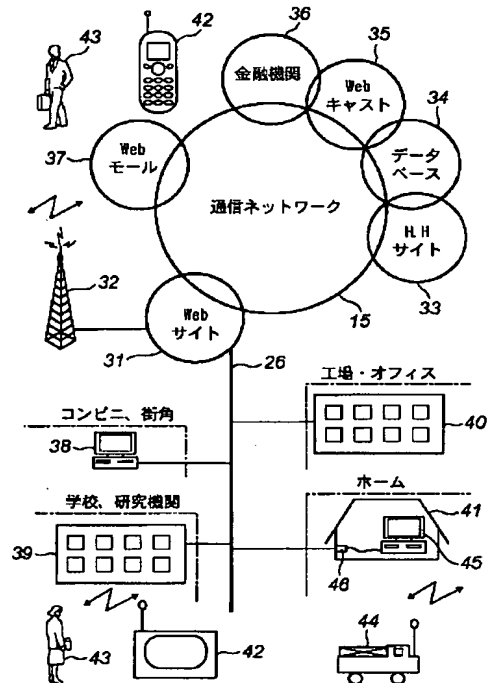
【図17】



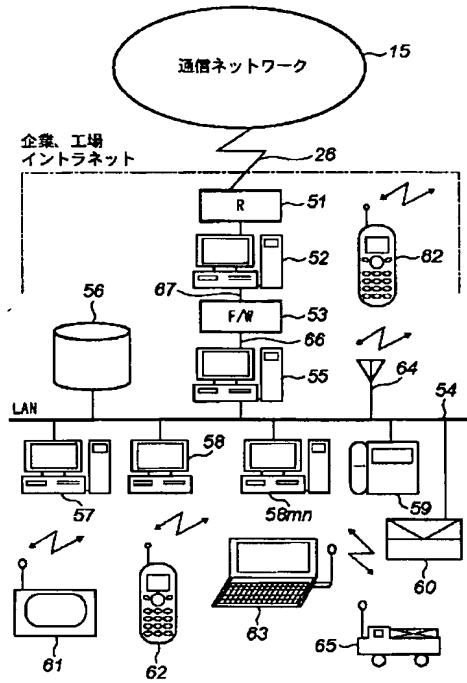
【図16】



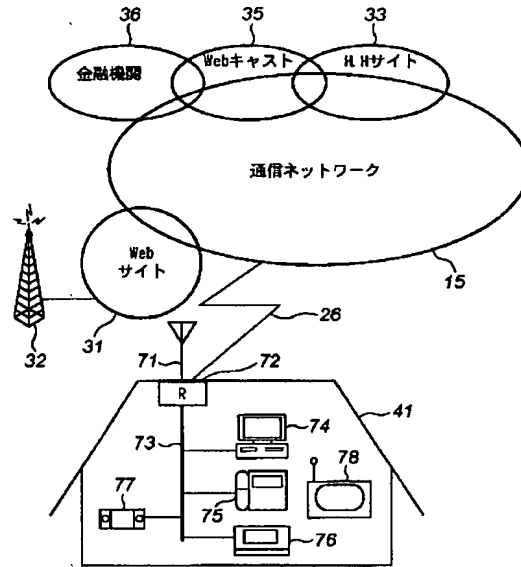
【図18】



【図19】



【図20】



【図21】

